AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE	OF	PAGES
	1		7

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
P00009	See Block 16B	PR201707210005	

6. ISSUED BY CODE

General Services Administration/FAS/ITC
Office of Acquisition Operations
1800 F Street, NW, 4th Floor
Washington DC 20405

7. ADMINISTERED BY *(If other than Item 6)* CODE

8. NAME AND ADDRESS OF CONTRACTOR

Harris Corporation
2400 Palm Bay Road NE
Palm Bay FL, 32905-3577

CODE FACILITY CODE

(☐) 9A. AMENDMENT OF SOLICITATION NO.

9B. DATED ***(SEE ITEM 11)***

(X) 10A. MODIFICATION OF CONTRACT/ORDER NO.
GS00Q17NSD3005

10B. DATED ***(SEE ITEM 13)***
7/31/2017

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is ☐ extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning __ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATA SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and data specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

N/A

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

(☐)	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation date, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: Mutual Agreement of Both Parties (FAR 43.103(a)(3))
	OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor _ is not, X is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

SEE CONTINUATION PAGES

Except at provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*	16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*
Antoinette Williams Contracts Manager	Timothy Horan Contracting Officer

15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
(Signature of person authorized to sign)	03/05/2019	*(Signature of Contracting Officer)*	

1. The purpose of this modification is to change Sections F, G, I and J of the contract.

2. The contract is modified as follows:

Section F

1. Section F.2.1 Table of Deliverables is changed to add a new deliverable ID 130.

130	J.2.10.3.1.2	J.2.10.3.1.2, row for adjustment_aggregated_tax	Adjustment Aggregated Tax AGF Inclusion Notice	Initial to GSA: NLT ATO Initial to Agency: At TO award Updates to GSA and Agency: Upon approval of associated BSS change (See Section G.5.5.1)	GSA CO, GSA COR, OCO and agency COR

Section G

2. The Simplified Acquisition Threshold referenced in Sections G.2.6 and 3.1 is changed from $150,000 to $250,000.
3. Section G.3.2 is modified to read “A TO will still be required for low-value orders that are under the fair opportunity threshold (see Section G.3.1).” vs “A TO will still be required for low-value orders that are under the fair opportunity threshold (see Section G.3.1), unless the order is funded entirely via a government purchase card (see Section G.4.8).”
4. Section G.5.3.1.3 is modified to delete the final bullet currently reading “BSS Verification Test Results”
5. Section G.8.2.1.1 is modified to read “The following table lists each service SLA and a reference to the appropriate location in Section C Technical Requirements. The referenced portion of Section C contains the associated KPIs, their definitions, measurement methodologies, and AQLs. The SLA is defined by all KPIs listed for the service in Section C except those for Time-to-Restore which are addressed in Section G.8.2.1.2.” vs “The following table lists each service SLA, the KPIs that define the SLA, and a reference to the appropriate location in Section C Technical Requirements. The referenced portion of Section C contains KPI definitions, their measurement methodologies, and their AQLs.”
6. Section G.8.2.1.1.1 the table is modified to delete the third column, labeled "KPIs Defining the Service-Specific SLA"
7. Section G.8.4.1 is modified after the first sentence of the second paragraph to insert the following: “For the billing accuracy SLA, defined in Section G.8.2.3, the six-month

window for SLACR submission shall begin at the end of the six-month holding period included in the underlying KPI definitions (see Sections G.4.12.1 and G.4.12.2)."

Section I

8. Add FAR Clause 52.204-23-Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018).

Section J

9. Section J.2.2 is modified to append a new subsection numbered J.2.2.5, titled "Empty Deliverables" and reading "Unless otherwise specified in the relevant contract section below or otherwise directed in accordance with Section J.2.2.3, the contractor shall submit all deliverables described in Section J.2 in accordance with the associated delivery timeframes even if the deliverable contains no data. If the deliverable is empty, i.e., it contains no data, the contractor shall submit a notice indicating that no data is available. Notwithstanding the delivery method indicated for the specific deliverable, this notice shall be sent via email to the GSA COR and, if the customer has previously requested receipt of the deliverable, to the customer OCO and COR. This notice is not required prior to the issuance of the first TO to the contractor."
10. Section J.2.3.3.1 is modified to delete the table row for Data Set Account Type
11. Section J.2.3.3.1 is modified to delete the table row for Data Set Delivery Type
12. Section J.2.3.3.1 is modified in table row for Data Set KPI Unit Type to read "KPI Unit Code" vs "KPI Unit Type"
13. Section J.2.3.3.1 is modified to delete the table row for Data Set Primary Interexchange Carrier
14. Section J.2.4.1.9, item 1 is modified to read "If the contractor splits an order such that separate suborders are used to provision services logically linked by a Service Grouping ID as described in Section J.2.10.1.1.2 Unique Billing Identifier, each such suborder shall have the same service order completion date reported in the associated SOCN" vs "Services logically linked by a Service Grouping ID as described in Section J.2.10.1.1.2 Unique Billing Identifier, shall not be split across multiple suborders"
15. Section J.2.4.1.9 is modified to append a new item to the numbered list reading "Each suborder must be processed fully as described in Section J.2.4.2.1 including issuing all required ordering data sets with the exception of the SORN which can only apply to the original order as issued by the government."
16. Section J.2.5.1.5.1.1, item 5 is modified to read "The billable amount for the service in that month (base_line_item_price) is equal to the daily charge from step 1 multiplied by the billable days from step 4: [Billable Amount] = [Daily Charge] x [Billable Days]" vs "The billable amount for the service in that month is equal to the daily charge from step 1 multiplied by the billable days from step 2: [Billable Amount] = [Daily Charge] x [Billable Days]"
17. Section J.2.5.1.5.1.2, item 6 is modified to read "The billable amount for the service in that month (base_line_item_price) is equal to the daily charge from step 1 multiplied by the billable days from step 4: [Billable Amount] = [Daily Charge] x [Billable Days]" vs "The billable amount for the service in that month is equal to the daily charge from step 1 multiplied by the billable days from step 2: [Billable Amount] = [Daily Charge] x [Billable Days]"

18. Section J.2.5.1.9 is modified in the fourth bullet (AGF Detail) to append “As this data set is submitted to GSA only, it shall be submitted at a contract level with each submission covering all TOs.”
19. Section J.2.5.1.9 is modified in the fifth bullet (AGF Electronic Funds Transfer Report) to append “As this data set is submitted to GSA only, it shall be submitted at a contract level with each submission covering all TOs.”
20. Section J.2.7.1 is modified to append a new subsection numbered J.2.7.1.4, titled “Reporting of Inventory Item UBIs” and reading “The inclusion of a UBI in the IR is dependent on the pricing mechanism of the inventory item it represents. A UBI representing an inventory priced as a Monthly Recurring Charge (MRC) or priced based on usage shall be included in the IR for the month of installation and all subsequent IRs through the IR for the month of disconnection. A UBI representing an inventory priced as a Non-Recurring Charge (NRC) shall be included in the IR for the month of installation and all subsequent IRs until the NRC is billed (i.e., included on the BI) but may be excluded from all IRs thereafter."
21. Section J.2.10.1.1.2.2, item 5 is modified to read “The contractor shall apply logical grouping when constructing the service grouping such that services ordered and used together or otherwise interdependent shall be grouped together (e.g., a circuit with originating and terminating ends and equipment at each end shall all be included in the same service grouping). This requirement may be satisfied by, at minimum, ensuring the same service grouping is used for all UBIs representing CLINs for the same instance of a single service as defined in Section C.1.8.1.” vs. “The contractor shall apply logical grouping when constructing the service grouping (e.g., a circuit with originating and terminating ends and equipment at each end shall all be included in the same service grouping).”
22. Section J.2.10.1.1.4.3.1 is modified to append the following: “Note: If the order cancellation is issued beyond the deadlines specified in Section G.3.3.2.3.1 and a cancellation CLIN is applied, the order update is handled as described in Section J.2.10.1.1.4.3.2 Line Cancellation.”
23. Section J.2.10.1.1.4.3.2 is modified to append the following: “Note: if the line cancellation update is issued beyond the deadlines specified in Section G.3.3.2.3.1 and a cancellation CLIN is applied, the contractor shall assign the line item order type "Add" to the cancellation CLIN.”
24. Section J.2.10.2.1.5 is modified in the table to read “quantity” vs “Quantity”
25. Section J.2.10.2.1.9 is modified in the column Value Requirement to read “If Applicable” vs “Always” for the following Element Names: agency_hierarchy_code, contract_line_item_number, clin_description, iconectiv_nsc
26. Section J.2.10.2.1.10 is modified to insert a paragraph before the table reading "Values for unique_billing_identifier, agency_hierarchy_code, contract_line_item_number, clin_description, and iconectiv_nsc may be omitted on data rows associated with the Billing Data Accuracy KPI (see Section G.4.12.1), the Billing Charges Accuracy KPI (see Section G.4.12.2), or the associated Billing Accuracy SLA (see Section G.8.2.3)."
27. Section J.2.10.2.1.10 is modified in the table row for Element Name contractor_service_request_number, column Value Requirement to read “If Applicable” vs “Always”
28. Section J.2.10.2.1.14, first bullet is modified to read "Although specified as 'If Applicable', values are always required for unique_billing_identifier, agency_hierarchy_code, and service except for the Billing Data Accuracy KPI (see Section G.4.12.1) and the Billing Charges Accuracy KPI (see Section G.4.12.2)." vs "Although specified as 'If Applicable', values are always required for 'unique_billing_identifier' and 'service' except for the

Billing Data Accuracy KPI (see Section G.4.12.1) and the Billing Charges Accuracy KPI (see Section G.4.12.2)."

29. Section J.2.10.2.1.14 is modified in the table row for Element Name agency_hierarchy_code, column Value Requirement to read “If Applicable” vs “Always”
30. Section J.2.10.2.1.18 is modified in the second bullet to read “province” vs “state”
31. Section J.2.10.2.1.18 is modified to insert a third bullet reading “If the location is in a country/jurisdiction with no legally recognized states or provinces, both location_state and location_province may be left blank.”
32. Section J.2.10.2.1.22 is modified in the table row for Element Name agency_hierarchy_code, column Value Requirement to read “If Applicable” vs “Always”
33. Section J.2.10.2.3.4 is modified in the table to read “service_id” vs “service_id_”
34. Section J.2.10.2.3.4 is modified in the table to read “country_jurisdiction_id” vs “country-jurisdiction_id”
35. Section J.2.10.2.3.5 is modified in the table to read “clin” vs “Clin”
36. Section J.2.10.2.3.5 is modified in the table to read “icb_number” vs “Icb_number”
37. Section J.2.10.3.1.1 is modified in the third bullet, fourth sub-bullet to append the following “; Negative values are preceded by a minus sign, ‘-’; Percentages are always converted to standard decimal values, e.g., 5% is presented as ‘0.05’”
38. Section J.2.10.3.1.1 is modified in the third bullet, sixth sub-bullet to read "(e.g., 13:05:30-04:00)" vs "(e.g., 13:05:30-4:00)"
39. Section J.2.10.3.1.1 is modified in the third bullet, seventh sub-bullet to read "(e.g., 2015-01-01T13:05:30-04:00)" vs "(e.g., 2015-01-01T13:05:30-4:00)"
40. Section J.2.10.3.1.1 is modified in the table row for Edit Mask Value HH:MM:SS+/-hh:mm, column Description to read "Example: 13:05:30-04:00" vs "Example: 13:05:30-4:00"
41. Section J.2.10.3.1.2 is modified in the table row for Element Name adjustment_aggregated_tax, column description to read “This is the total adjustments to all taxes, fees, and surcharges including the AGF. This value may omit the AGF at the contractor’s discretion provided they provide notice of their choice to their GSA CO and COR and the OCO and COR(s) associated with any awarded TOs. A minus sign indicates the charge is being reduced (i.e., a credit to the agency). If the charge is increased (i.e., a debit to the agency), no indicator is required.” vs “Adjustment to aggregated tax”
42. Section J.2.10.3.1.2 is modified in the table row for Element Name adjustment_amount, column description to read “This is the total line item amount of the adjustment including individual adjustments to CLIN price, AGF collected, taxes, fees and surcharges. A minus sign indicates the charge is being reduced (i.e., a credit to the agency). If the charge is increased (i.e., a debit to the agency), no indicator is required.” vs “Amount of adjustment”
43. Section J.2.10.3.1.2 is modified in the table row for Element Name adjustment_detail_tax_billed, column description to read “There are two allowed methods for supplying this data. Method 1: Provide a single line item which is the total adjustments to all taxes, fees, and surcharges normally reported in the TAX detail deliverable. This excludes the AGF. Under this method, tax_item_number is left blank unless otherwise specified in the Task Order (TO). Method 2: Provide individual line items for each adjusted tax, fee, or surcharge normally reported in the TAX detail deliverable. This excludes the AGF. Under this method, tax_item_number is populated with the appropriate value from the Allowable Taxes (ALLTAX) reference table. A minus sign indicates the charge is being reduced (i.e., a credit to the agency). If the charge is increased (i.e., a debit to the agency), no indicator is required.” vs “Adjustment detail of the aggregated tax”

44. Section J.2.10.3.1.2 is modified in the table row for Element Name adjustment_outcome, column Length to read “25” vs “255”
45. Section J.2.10.3.1.2 is modified in the table row for Element Name adjustment_outcome, column Edit Mask to insert “Ref: ADJOUT.code”
46. Section J.2.10.3.1.2 is modified in the table row for Element Name adjustment_reason, column Length to read “25” vs “255”
47. Section J.2.10.3.1.2 is modified in the table row for Element Name adjustment_reason, column Edit Mask to insert “Ref: ADJRSN.code”
48. Section J.2.10.3.1.2 is modified in the table row for Element Name charging_unit_code, column Length to read “5” vs “10”
49. Section J.2.10.3.1.2 is modified in the table row for Element Name contractor_charge_waiver_code, column Description to append the following “If the charge is being waived, the base_line_item_price may be reported as either its normal value or as zero (0) as agreed between the contractor and the customer or as indicated in the TO.”
50. Section J.2.10.3.1.2 is modified in the table row for Element Name contractor_direct_billed_agf_adjustment, column description to append “A minus sign indicates the charge is being reduced (i.e., a credit to the agency). If the charge is increased (i.e., a debit to the agency), no indicator is required.”
51. Section J.2.10.3.1.2 is modified in the table row for Element Name data_transaction_code, column Length to read “6” vs “10”
52. Section J.2.10.3.1.2 is modified in the table row for Element Name gsa_account_number is deleted
53. Section J.2.10.3.1.2 is modified in the table row for Element Name key_performance_indicator_measurement, column Description to read “This is the name of the KPI specified in a manner that is intended to be easily understood by CORs and other agency representatives (e.g., ‘Latency in continental US (CONUS)’, ‘Service Provisioning’, etc.)" vs “Name of the KPI (e.g., Availability)”
54. Section J.2.10.3.1.2 is modified in the table row for Element Name key_performance_indicator_unit_type_code, column Length to read “6” vs “20”
55. Section J.2.10.3.1.2 is modified in the table row for Element Name originating_location_country, column Type to read “Alpha” vs “Alphanumeric”
56. Section J.2.10.3.1.2 is modified in the table row for Element Name service_connect_end_date_and_time, column Length to read “25” vs “22”
57. Section J.2.10.3.1.2 is modified in the table row for Element Name service_connect_start_date_and_time, column Length to read “25” vs “22”
58. Section J.2.10.3.1.2 is modified in the table row for Element Name service_outage_cleared_date_&_time, column Length to read “25” vs “22”
59. Section J.2.10.3.1.2 is modified in the table row for Element Name service_outage_occurred_date_&_time, column Length to read “25” vs “22”
60. Section J.2.10.3.1.2 is modified in the table row for Element Name terminating_location_country, column Type to read “Alpha” vs “Alphanumeric”
61. Section J.2.10.3.1.2 is modified in the table row for Element Name time_of_state_change, column Length to read “25” vs “22”
62. Section J.2.10.3.2.1, fourth bullet, fourth sub-bullet is modified to insert the following “; Negative values are represented by preceding the number with a minus sign, ‘-’; Percentages are always converted to standard decimal values, e.g., 5% is presented as ‘0.05’”
63. Section J.2.10.3.2.2 is modified in the table row for Data Transaction Code ALLTAX and Element Name effective_date, column Length to read “25” vs “22”

64. Section J.2.10.3.2.2 is modified in the table row for Data Transaction Code ALLTAX and Element Name end_date, column Length to read “25” vs “22”
65. Add DFARS Clause 252.239-7010 Cloud Computing Services (OCT 2016) to J.18.

3. The estimated dollar value of the contract remains unchanged.

4. Except as provided herein, all prices, terms and conditions of the document referenced in Item 10A remain unchanged and in full force and effect.

Enterprise Infrastructure Solutions (EIS) Contract

Section B
Supplies or Services and Prices/Costs

Issued by:

General Services Administration

Office of Information Technology Category

[redacted]

~~January~~ June 2018

Table of Contents

B.1 Pricing Overview

B.1.1 Overview

This section defines price tables and other pricing mechanisms for the services and features described in Section C. All prices shall conform to the format and structure defined herein. Additional price elements not included in the defined format and structure are not permitted, except as defined in separate TOs awarded under this contract. All prices and price elements defined under this contract or defined under TOs shall conform to the pricing requirements, specifications, element definitions, and numbering schemes defined in this contract.

Contract prices and price tables define the permitted charges and charging schemes. Pricing mechanisms defined for TOs must be derived from (i.e., logically flow from) contract price tables. Examples of such price mechanisms and elements associated with TO pricing may include, but are not limited to, the following:

1. Pricing mechanisms identical to those in the contract, except for additional pricing discounts or reductions negotiated under the TO competition.
2. Prices for multiple contract elements or TO elements combined under a single price element (e.g., single price for service plus Service Related Equipment (SRE), so-called “solutions,” or a special labor skill need).
3. Pricing for services, SRE, or labor, that vary from the contract in some significant aspect, such as higher performance levels, additional features, or a special security service labor requirement.
4. Individual Case Basis (ICB) pricing.
5. Task Order Unique CLINs (TUCs).

All prices agreed to at the contract award are established for all contract users (e.g., agencies/customers). Agencies and/or customers are expected to conduct one or more fair opportunity actions that will result in the award of TOs under this contract.

Where price elements awarded under a TO differ from contract pricing, the contractor shall associate the TO number with each CLIN and price element awarded that differs from contract pricing. For more information, see Section B.1.2.16.

The contractor shall not process orders nor will the government pay invoices until the contractor has submitted these prices into GSA Systems (see Section J.2.3). The contractor shall submit into GSA Systems a copy of the resulting TO for purposes of validating the orders, bills and invoices as defined in Section J.2. For a complete description of the ordering requirements, refer to Section G.3.

B.1.2 General Pricing Principles

Pricing for telecommunications and networking services historically has been complex, due in large part to regulatory requirements. Simpler pricing approaches are expected for the future. Such pricing simplification is already being seen in residential and commercial pricing trends for combined services such as voice and data. Services based on legacy copper wire and circuit switching will be retired in the next few years. Accordingly, price tables and elements defined in this section reflect a hybrid of complex legacy and simpler modern pricing mechanisms. As providers retire legacy infrastructure, agencies will modernize their networks and applications, reducing pricing, ordering, and billing complexities. EIS seeks to provide an orderly path to future pricing by accommodating current legacy services pricing while allowing for the evolution of future services pricing toward greater flexibility and simplicity. This approach is expected to result in fewer pricing elements and greater pricing transparency.

Critical to the EIS approach is allowing (but not requiring) the network engineered access topography to be decoupled from pricing. This is accomplished by allowing common access prices to be defined for services and service groupings regardless of location or access engineering, which allows for fewer pricing points and simpler price structures. Legacy services may continue to be priced as in the past. Access pricing is described in Section B.2.9.

B.1.2.1 Service Areas, Services and References

Service areas refer to collections of related telecommunications services, plus discrete areas to be priced such as labor and equipment. Services refer to the components of the service areas.

The following service areas are defined in Section C.2:

1. Data Service
2. Voice Service
3. Contact Center Service
4. Colocated Hosting Service
5. Cloud Service
6. Wireless Service
7. Commercial Satellite Communications Service
8. Managed Services
9. Access Arrangements
10. Service Related Equipment

11. Service Related Labor
12. Cable and Wiring

The National Security and Emergency Preparedness requirements are defined in Sections C.1.8.8 and G.11.

Table B.1.2.1.1 defines the structure for service areas and services. The table also defines which services are mandatory (to be included in the contractor's proposal), and which services are optional. Refer also to Section C.2.1 for a discussion of mandatory and optional services.

B.1.2.1.1 Pricing Identification Structure

Service Area	Service Name	Mandatory/ Optional (M/O)	Service ID	Service CLIN Prefix	Section C Reference	Section B Reference	CBSA Based Service*
Data Service	Virtual Private Network Service	M	VPNS	VN	C.2.1.1	B.2.1.1	Yes (One-sided)
	Ethernet Transport Service	M	ETS	EN	C.2.1.2	B.2.1.2	Yes (One-sided for E-LAN and Two-sided for E-LINE)
	Optical Wavelength Service	O	OWS	OW	C.2.1.3	B.2.1.3	Yes (Two-sided)
	Private Line Service	O	PLS	PL	C.2.1.4	B.2.1.4	Yes (Two-sided)
	Synchronized Optical Network Service	O	SONETS	SO	C.2.1.5	B.2.1.5	Yes (Two-sided)
	Dark Fiber Service	O	DFS	DK	C.2.1.6	B.2.1.6	Yes (Two-sided)
	Internet Protocol Service	O	IPS	IP	C.2.1.7	B.2.1.7	Yes (One-sided)
Voice Service	Internet Protocol Voice Service**	M	IPVS	VI	C.2.2.1	B.2.2.1	Yes (One-sided)
	Circuit Switched Voice Service**	M	CSVS	VS	C.2.2.2	B.2.2.2	Yes (One-sided)
	Toll Free Service	O	TFS	TF	C.2.2.3	B.2.2.3	Yes (One-sided)
	Circuit Switched Data Service	O	CSDS	CS	C.2.2.4	B.2.2.4	Yes (One-sided)
Contact Center	Contact Center Service	O	CCS	CC	C.2.3	B.2.3	No
Colocated Hosting Service	Colocated Hosting Service	O	CHS	CH	C.2.4	B.2.4	No
Cloud	Infrastructure as a Service	O	IaaS	IA	C.2.5.1	B.2.5	No
	Platform as a Service	O	PaaS	PA	C.2.5.2	B.2.5	No
	Software as a Service	O	SaaS	SS	C.2.5.3	B.2.5	No
	Content Delivery Network Service	O	CDNS	CD	C.2.5.4	B.2.5.3	No
Wireless	Wireless Service	O	MWS	WL	C.2.6	B.2.6	No
Commercial Satellite Communications Service	Commercial Mobile Satellite Service	O	CMSS	CM	C.2.7	B.2.7.1	No
	Commercial Fixed Satellite Service	O	CFSS	FS	C.2.7	B.2.7.2~~B.2.7.2~~	No

Formatte

Service Area	Service Name	Mandatory/ Optional (M/O)	Service ID	Service CLIN Prefix	Section C Reference	Section B Reference	CBSA Based Service*
Managed Services	Managed Network Service	M	MNS	MN	C.2.8.1	B.2.8.1	Yes (One-sided)
	Web Conferencing Service	O	WCS	WC	C.2.8.2	B.2.8.2	No
	Unified Communications Service	O	UCS	UC	C.2.8.3	B.2.8.3	Yes (One-sided)
	Managed Trusted Internet Protocol Service	O	MTIPS	MT	C.2.8.4	B.2.8.4	Yes (One-sided)
	Managed Security Service	O	MSS	MS	C.2.8.5	B.2.8.5	Yes (One-sided)
	Managed Mobility Service	O	MMS	MM	C.2.8.6	B.2.8.6	No
	Audio Conferencing Service	O	ACS	AC	C.2.8.7	B.2.8.7	No
	Video Teleconferencing Service	O	VTS	VC	C.2.8.8	B.2.8.8	No
	DHS Intrusion Prevention Security Service	O	IPSS	DI	C.2.8.9	B.2.8.9	No
Access Arrangements	Access Arrangements***	M	AA	AA	C.2.9	B.2.9	Yes (One-sided)
Service Related Equipment	Service Related Equipment	O	SRE	EQ	C.2.10	B.2.10	Yes (One-sided)
Service Related Labor	Service Related Labor	O	LABOR	LA	C.2.11	B.2.11	Yes (One-sided)
Cable and Wiring	Cable and Wiring	O	CW	CW	C.2.12	B.2.12	Yes (One-sided)
National Security and Emergency Preparedness**	National Security and Emergency Preparedness		NS/EP	NS	C.1.8.8 / G.11	B.3	No
General	General	O	GEN	GN		B.4.1.13, B.4.1.14	

* Services identified with a Yes (One-sided) may only be provisioned in awarded CBSAs; services identified with "Yes" (Two-sided) may only be provisioned between two awarded CBSAs. Services identified with "No" may be provisioned where priced (e.g., CONUS, OCONUS, non-domestic).

** The contractor shall propose prices for at least one of the two Voice services. If prices for both are provided, the contractor shall indicate by CBSA which one the government is to regard as the mandatory service.

*** Access arrangements are required where the contractor proposes service. Section J.1.3 provides the geographic requirements for access.

**** NS/EP is listed in this table and is not a service but rather a required set of mandatory CLINs. In the AcquServe portal, the contractor shall select National Security and Emergency Preparedness in the EIS Service Selection tool and shall price the required NS/EP CLINs from B.3.2.2.

B.1.2.1.1.1 CLINs and Features

Each permissible individual pricing element is identified by a Contract Line Item Number (CLIN)[1]. Each CLIN is a seven-character identifier, the first two characters of which identify the service, as shown in the Service CLIN Prefix column in Table B.1.2.1.1. The referenced subsections for each service contain further CLIN discussion and definitions.

Services, as defined in this contract for pricing purposes, may include "standard features" that do not have separate CLINs. Additional features may be separately identified, ordered, and priced. Such features are identified by a separate CLIN. Their prices may be zero (i.e., not separately priced (NSP)) or non-zero.

Features are addressed in the sections identified for each service in Table B.1.2.1.1.

B.1.2.2 Service Pricing Elements and Conditions

All services will have either defined fixed prices or ICB price elements, except where previously unanticipated pricing types are needed, such as the following:

- A bandwidth that is not listed on the contract, but logically should be added and defined on the contract as a fixed price item. For example, if CLINs for 10 Mbps, 20 Mbps, and 40 Mbps are defined, but the agency requires a 30 Mbps CLIN, then this 30 Mbps CLIN shall be added to the contract with a fixed price prior to the TO.
- A bandwidth that is not listed on the contract, but logically should be added and defined on the contract with an ICB CLIN. For example, if CLINs for OC12 and OC192 access are defined, but the agency requires an OC48 access CLIN, then it shall be added to the contract prior to the TO.
- A new item that does not fall into any of the fixed or ICB CLINs for that service. In this instance, the agency and the contractor shall use the TUCs defined for the specific service. A new CLIN is not required for the contract. See Sections B.1.2.12 and B.1.2.15 for further information.

Any equipment, material, facility, labor, site preparation, training, or other service required in the performance of this contract for which a price is not specifically identified in the contract will be considered to be included in the price of another item or provided at no cost to the government, except as otherwise provided for in this contract or the

[1] Additional information may be required to determine a price; for example, location information is required to determine access prices (see Section B.2.9).

applicable TO. The contractor may waive any charge at any time. No charges are permitted for interconnection with a government provided circuit at a contractor's POP. Prices for any associated SRE shall be provided in accordance with Section B.2.10.

The following conditions also apply to prices and price structures:

- Prices shall be specified and billed in United States (U.S.) currency.
- Prices populated in Section B price tables shall have a maximum of two (2) decimal places, except for prices associated with CLINs that are priced using charging units of a particularly small measure (e.g., per minute, per six-second or per second), which shall have a maximum of six (6) decimal places. The maximum number of decimal places for each charging unit is defined in the price precision column of the "unit" reference table. In addition, at least six (6) decimal places shall be carried in all calculations up to final rounding. See Section J.2.5.1.6 for a discussion of rounding.
- All mandatory CLINs for mandatory services shall be offered by the contractor, including Individual Case Basis (ICB) items that will be instantiated as CLINs when priced. These mandatory ICB CLINs are not part of the contract as orderable CLINs until priced and added to the TO. Until then, these ICB CLINs represent place-holders for specific priced CLINs so that the service being proposed may be defined and associated with a unique identifier. ICB elements require additional information to fully specify the prices involved. This information shall be provided by the contractor in the format provided in GSA Systems. In this system, the contractor shall provide the anticipated CLIN, ICB Case Number, Case Description, Charging Unit, and, where applicable, the Network Site Code and Country Jurisdiction ID, in Table B.1.2.14.1. The Case Description shall contain sufficient information to distinguish one case from another of the same CLIN. Customers will use this description to assist in their evaluations.
- The ICB CLIN, Case Number, Description, Charging Unit, and Price are instantiated in the TO. The Case Number shall be unique for each CLIN and Case.
- Where service is distinguished between routine and critical, it is assumed that the fixed prices proposed are for routine service. Pricing for critical service levels will be obtained as specified in the TO. The critical service obtained in the TO will include one or more of the following:
    - Existing diversity CLINs
    - ICB CLINs

- TUCs

- If a contractor proposes optional services, it shall offer the mandatory CLINs associated with those services.
- If a contractor proposes an NSP CLIN, the contractor shall populate the price table with a price of $0 for that CLIN.
- Prices shall be fixed for all services, features, and labor for each applicable fiscal year within the contract period.
- All prices proposed shall exclude the Associated Government Fee (AGF).

B.1.2.3 Effective Pricing Dates

The contractor shall maintain all price tables for the full contract period. All prices shall be binding at the time of the effective date of the contract. For prices that are effective later than contract award, the contractor shall define the day, month, and year in which the prices are to become effective. The contract shall be for a base period of 60 months, with two (2) option periods of 60 months each. Prices shall be specified for the base period. Pricing shall change only on the first day of the U.S. Government fiscal year, except as provided below.

All prices on a row of a price table shall carry a start date, which is when the prices on that row become effective and the service becomes available. These prices shall remain in effect through their listed price stop date or until the prices are changed by modification[2]. When prices are revised by modification, the newly inserted rows shall include the start date(s) when the prices become effective. If a service is ordered for delivery on or after the price start date (but before the stop date) shown on the price table row, the contractor shall provide the service at the accepted price, subject to the conditions identified in Section J.1.

Thereafter, the billed price shall be obtained from the price table row within which the billing date is contained. The only exception to this rule is the SRE MRC, for which the billed price for the duration of the SRE MRC payment term is fixed at the time of the order. The same rules regarding price table row start dates and stop dates shall apply to the start dates and stop dates for all price tables (e.g., cross-reference tables, Point of Presence (POP) identification tables, and POP relationship tables). See Section B.4 for additional information. See Section J.4 for information on the modification process.

[2] Modifications can take the form of contract modifications, TO-specific submissions, or catalog submissions.

Upon award of the contract within a Government fiscal year, the prices for contract pricing year 1 shall be effective from the award date through September 30 of that Government fiscal year. The prices for contract years 2 through 5 will remain on a Government fiscal year basis. The prices for contract pricing year 6 shall be effective from October 1 of the last fiscal year of the 60 month base period through the last day of the 60 month base period.

Upon contract award, the government will update each contractor's price tables to change the first start date to the award date, and the last stop date to the corresponding last day of the 60 month base period.

B.1.2.4 Price Banding Structures

Some tables permit prices to be defined by bands (e.g., by distance or bandwidth). Each band is defined by a "Band Low" and a "Band High". Where the contractor is permitted to define bands, the bands shall be contiguous with no overlapping bands or gaps between bands.

To ensure that bands are contiguous, each "Band High" shall be identical to the "Band Low" of the subsequent band. Using this convention, each band shall include the entire interval from "Band Low" up to, but not including, "Band High" except for the last band in a given table, where the "Band High" shall be included.

Each banded price table shall include a row where Band Low = 0.

Price banding can be used for fixed price and variable price components applied separately or in combination in a given price table:

- With fixed price banding, the banded value serves as an index into the price table to select the correct row, and then the value in the fixed price column of that row is used as the CLIN price.
- With variable price banding, the banded value serves as an index into the price table to select the correct row, and then the value in the variable price column of that row is multiplied by the banded value to arrive at the CLIN price.

MRC CLIN	Case Number	Task Order Number	Band Low	Band High	Fixed Price	Variable Price	Price Start Date	Price Stop Date
XX00001			0	10	$350	$85	10/1/2016	9/30/2021
XX00001			10	200	$300	$80	10/1/2016	9/30/2021
XX00001			200	1000	$200	$50	10/1/2016	9/30/2021

In the example above, the fixed and variable price components are used in combination to calculate the MRC.

Assuming the quantity of CLIN XX00001 for the month is 10, then the price calculation for that CLIN is the fixed component for that band – $300 in this case, plus the variable component – in this case $80 per unit of the CLIN, or $800 for the month. The total price is $300 + $800 = $1,100.

Alternatively, if the quantity of CLIN XX00001 for the month is 250, then the price for that CLIN is $200 fixed, plus $50 per unit of the CLIN, or $12,500. The total price for this item is $200 + $12,500 = $12,700 for the month.

If the Variable Price column had not been included in the table above, then the MRCs would be $300 and $200, respectively. If the Fixed Price column had not been included in the table above, the MRCs would be $800 and $12,500, respectively.

B.1.2.5 Pricing Domestic and Non-Domestic Locations

Prices for telecommunications services as defined in Table B.1.2.1.1 shall provide geographic coverage for domestic and non-domestic locations, as specified in Section J.1. Domestic wireline locations are further divided into CONUS and OCONUS as defined in Section J.12. Prices for wireline access for service at non-domestic locations, except as otherwise included in transport pricing, shall be provided in fixed price tables. Domestic wireless locations are defined in Section B.2.6.

No pass-through pricing shall be allowed for any service. Pass-through charges are defined as the actual cost of the service without markup, overhead, or profit.

Non-domestic calls are classified as:

- Outbound – calls made from a domestic service delivery point (SDP) to a non-domestic location
- Inbound – calls made from a non-domestic location to a domestic location
- Non-domestic-to-non-domestic – calls made from one non-domestic location to another non-domestic location

All non-ICB CLINs listed in price tables that do not have Country/Jurisdiction ID or Pricing Hub (PHub) ID columns shall apply to all locations, and shall be offered at the stated fixed price where offered commercially by the contractor. See Section J.1 for non-domestic coverage requirements.

B.1.2.6 Price Factors and CLINs

The fixed prices for services may depend on a number of factors, including but not limited to:

1. Geographic location
2. Access type
3. Types of data service port requirements as defined in the individual service sections in Section C
4. Types of services and features provided
5. Distance[3]

The total basic service price for a connection will consist of various CLINs, with the number and types of CLINs being dependent on the mix of conditions associated with the service. Basic service prices will vary by service type and are described in more detail in the individual service pricing sections. Prices for services may include, but are not necessarily limited to, the following components:

1. Non-Recurring Charges (NRC) for access and priced features (see B.2.9 for access pricing)
2. Monthly Recurring Charges (MRC) for flat rate charges, cloud services, access, transport, and priced features
3. SRE charges
4. Service Related Labor charges
5. Usage-based charges for access, transport, cloud services, and priced features
6. ICB charges for customized or unique requirements. ICB prices are determined as needed and specified in TOs (see Section B.1.2.14).

Domestic access prices and domestic transport prices shall be unbundled except as otherwise provided (e.g., VPNS CLINs that bundle access with the transport, or CLIN bundling per Section B.1.2.12).

B.1.2.7 Use of Geographic Coordinates and POPs

For domestic locations, all distance[4] measurements shall be calculated using Vertical and Horizontal (V&H) coordinates. The V&H coordinates of a Physical Concentration

[3] Where distance-sensitive pricing is provided in the form of distance bands, these distance bands shall be contiguous.
[4] The distance between two locations shall be calculated in miles as:
Distance (miles) = ROUNDUP(SQRT(((V1-V2)^2+(H1-H2)^2)/10),0)
Where (V1, H1) and (V2, H2) are the V and H coordinates of the locations, respectively.

Location (PCL), such as a serving wire center, fiber hotel or cable head, shall be provided by the contractor. The V&H coordinates of POPs shall be provided and maintained by the contractor. In tables and other documents prepared for the government, distances shall be reported in miles.

Price tables for transport (i.e., POP-to-POP transmission) for services are defined in the individual service subsections in Section B.2. Transport prices are for the transmission of information, including voice, data, video, and/or multimedia, across the network.

Domestic transport distance is measured between the POPs that are designated for the on-net or off-net locations. The price for transport between a domestic location and a non-domestic location or between a non-domestic location and another non-domestic location is computed on a country/jurisdiction-to-country/jurisdiction basis (except as otherwise provided for), with the locations in the domestic definition divided into separately identified regional groupings (each with its own Country/Jurisdiction ID for transport pricing purposes). See Table B.4.2.1.

The formats for domestic POPs and non-domestic POP locations are listed in Section B.4.1. Table B.4.1.5 identifies bandwidth groups available at each PCL and maps PCLs to POPs. No PCL shall map to more than one POP for any assigned bandwidth group. For each service provided at a POP in Table B.4.1.1, all bandwidth groups identified for that service shall be available at any PCL mapped to that POP for those bandwidth groups. Each POP shall provide all bandwidth groups from all PCLs mapped to that POP. POPs may be added or deleted at any time during the term of the contract; however, no increase in access arrangement pricing shall be permitted. The contractor shall give a minimum of six months' notice of such a change, except in the case of emergency conditions.

B.1.2.8 Waiver of Charges

The contractor may waive the application of any charges at any time during the contract period, including during transition to EIS.

B.1.2.9 Pricing Volume

The contractor's Pricing Volume shall be incorporated at award. The contractor shall provide updates throughout the life of the contract as needed to assure a clear, unambiguous understanding of pricing methods. Any significant change to the pricing methodology should be reflected. Examples include, but are not limited to:

- The introduction of new services
- Allowable changes to pricing methodologies
- End of Life services

If the contractor fails to clearly define a pricing method for any service, then the government's interpretation shall apply. Refer to Section F for other deliverable requirements.

B.1.2.10 Usage Based Charges

The contractor shall round up usage based charges if the billable measurement exceeds the unit. For example, for usage billing in six-second increments, a seven-second call will round up usage to 12 seconds. For usage billing in one-minute increments, a 61 second call will be rounded up to two minutes for billing purposes.

B.1.2.11 Auto-Sold CLINs

Some services include other CLINs that the contractor automatically includes with those services. For example, conferencing customers may request any of the features associated with a contractor's specific conferencing services.

The contractor shall not auto-sell SRE.

A comprehensive list of auto-sold CLINs (which may include catalog items) shall be incorporated into Table B.1.2.11.1. As new capabilities and features are added to the contract for the services that have auto-sold CLINs (such as Audio, Web and Video Conferencing), contractors shall update Table B.1.2.11.1. Contractors shall populate Table B.1.2.11.1 with, at a minimum, the CLIN-to-Auto-sold CLIN relationships listed in reference table B.1.2.11.2 for:

- VPNS and ETS
- IPS, if the optional service IPS is offered

B.1.2.11.1 Auto-Sold CLINs Table

CLIN*	CLIN Case Number**	Auto-Sold CLIN***	Auto-Sold CLIN Case Number**	Task Order Number****	Start Date	Stop Date

* All CLINs within Section B that have auto-sold CLINs
** If the CLIN or Auto-Sold CLIN is not ICB, populate the corresponding case number column with -1
*** CLINs which are auto-sold with the base CLIN
**** A row where the Task Order Number = -1 shall apply to all task orders. A row where the Task Order Number column is populated with a specific agency task order shall, for that task order only, disable the auto-sold relationship defined by that row.

B.1.2.11.2 Auto-Sold Mandatory Relationships Reference Table

Service ID	CLIN	Auto-Sold CLIN
VPNS	VN30001	VN30009
VPNS	VN30002	VN30009
VPNS	VN30003	VN30009
VPNS	VN30004	VN30009
VPNS	VN30005	VN30009
VPNS	VN30010	VN31020
VPNS	VN30011	VN31030
VPNS	VN30012	VN31040
VPNS	VN30013	VN31050
VPNS	VN30021	VN31200
VPNS	VN30022	VN31300
VPNS	VN30023	VN31400
VPNS	VN30024	VN31500
VPNS	VN30025	VN31600
ETS	EN30010	EN31020
ETS	EN30011	EN31030
ETS	EN30012	EN31040
ETS	EN30013	EN31050
ETS	EN30014	EN31200
ETS	EN30015	EN31300
ETS	EN30016	EN31400
ETS	EN30017	EN31500

Service ID	CLIN	Auto-Sold CLIN
ETS	EN30018	EN31600
IPS	IP30001	IP30008
IPS	IP30002	IP30008
IPS	IP30003	IP30008
IPS	IP30004	IP30008
IPS	IP30005	IP30008
IPS	IP30010	IP40020
IPS	IP30011	IP40030
IPS	IP30012	IP40040
IPS	IP30013	IP40050
IPS	IP30021	IP40200
IPS	IP30022	IP40300
IPS	IP30023	IP40400
IPS	IP30024	IP40500
IPS	IP30025	IP40600

B.1.2.12 CLIN Bundling

Agencies may desire to combine multiple contract CLINs and/or TUCs into a single TUC. For example, an agency may wish to bundle a VPNS Port CLIN, MNS CLIN, and SRE into one combined CLIN. In these instances, the contractor shall provide items that have been combined for a specific TO in Table B.1.2.12.1, to facilitate the collection of the components necessary for an accurate inventory. A combined TUC shall not contain multiple component CLINs for transport (e.g., combining 50 Mbps VPNS with 100 Mbps VPNS), or multiple component CLINs for Access Arrangements. All component CLINs bundled into a single TUC must use the same billing frequency. A combined TUC defined in Table B.1.2.12.1 shall be priced using the TUC price table of the transport service that is bundled into that combined TUC and shall not be priced using General TUC Prices Table B.4.1.14.1.

B.1.2.12.1 TUC Combined CLIN Component Table

CLIN*	Case Number	Task Order Number	Component CLIN**	Component CLIN Case Number***	Component Access PHub ID****	Component SRE Pricing Element***	Component CLIN Quantity	Start Date	Stop Date

* From the appropriate TUCs of the basic transport service for the combined CLIN set (e.g., VPNS)
** Component CLINs associated with the combined TUC. A separate row shall be used for each component CLIN
*** Where applicable, otherwise "-1"
**** Where applicable, otherwise null

B.1.2.13 Adding CLINs Post-Award

Contractors may submit proposals for contract modifications post-award (see Section J.4) and define new CLINs using Table B.1.2.13.1, which includes:

- **Name** – the description of the specific service provided under the CLIN
- **Frequency** – the billing frequency – "NRC", "MRC" or "Usage"
- **ICB** – "T" if the CLIN is priced on an individual case basis, "F" otherwise
- **NSP** – "T" if the CLIN is not separately priced, "F" otherwise
- **Unit ID** – the charging unit ID from the "unit" reference table
- **Notes** – contains any additional information that might be useful to understand the service defined by the CLIN

B.1.2.13.1 CLIN Table

CLIN	Name	Frequency	ICB	NSP	Unit ID	Notes

B.1.2.14 Defining New ICB Cases

Contractors shall define new ICB cases for which they submit pricing (see Section J.4). Contractors shall use Table B.1.2.14.1 to define ICB cases for TOs that use an ICB CLIN. Contractors shall ensure that NSCs and Country/Jurisdiction IDs in Table B.1.2.14.1 are the same as the values in the corresponding columns of the price table(s) used to price the CLIN and case number. Contractors shall populate the Terminating NSC and Terminating Country/Jurisdiction ID columns of Table B.1.2.14.1 with null values for cases where those location elements are not relevant.

B.1.2.14.1 General ICB Information Table

CLIN	Case Number	Case Description*	Task Order Number	Unit ID	Originating NSC**	Terminating NSC***	Originating Country/ Jurisdiction ID**	Terminating Country/ Jurisdiction ID****	Start Date	Stop Date

* For catalogs, this column is not used and shall be populated with "N/A" – the catalog description column takes precedence

** Where applicable, otherwise "-1"

*** Used only when the price table specifically identifies the NSC as a Terminating NSC

**** Used only when the price table specifically identifies the Country/Jurisdiction ID as a Terminating Country/Jurisdiction ID

In CLIN Table B.1.2.13.1, the Unit ID for an ICB CLIN shall function as a placeholder or recommended charging unit until a specific ICB case is defined using General ICB Information Table B.1.2.14.1. If no recommended charging unit is readily apparent for the ICB CLIN, the contractor shall populate the Unit ID column of CLIN Table B.1.2.13.1 with "73" to designate the charging unit as ICB. When a specific case is defined using General ICB Information Table B.1.2.14.1, the Unit ID in Table B.1.2.14.1 shall determine the charging unit used to calculate the price for that case and shall be chosen to specify as precisely as possible the unit of measure for the corresponding price. Unit ID 73 shall not be used in Table B.1.2.14.1.

B.1.2.15 Task Order Unique CLINs

As stated in Section B.1.2.2, TUCs are to be used for custom solutions not otherwise defined and priced on the contract. They allow pricing and ordering of such solutions without requiring a contract modification. Only the TUCs that are predefined for each service shall be used by agencies for ordering. Three types of TUCs are typically defined per service: MRC, NRC, and usage-based. All TUCs are priced as ICB CLINs.

When agencies and contractors define the technical and performance requirements for a custom solution, they shall include ICB descriptions for any associated TUCs. Multiple TUCs may be specified on a TO.

TUCs are also used for CLIN bundling as described in Section B.1.2.12.

B.1.2.16 Task Order Number Columns

Contractors shall populate the Task Order Number column of price tables with one of the following options:

- The value “-1” for contract pricing[5]
- The specific agency TO number for TO-specific pricing

B.1.2.17 Table Types

Section B uses four types of tables to support service pricing. Two of the table types are maintained by the contractor and the other two are maintained by the government.

B.1.2.17.1 Contractor-Maintained Tables

Price Tables contain prices by CLIN, TO number, date, and, where applicable, other pricing elements such as case number, location and price bands. Each price table specifies the pricing elements required for the particular service.

Supporting Tables do not contain prices but they contain other information that is required to price services. Examples include General ICB Information Table B.1.2.14.1, TUC Combined CLIN Component Table B.1.2.12.1, Auto-Sold CLINs Table B.1.2.11.1, and Services Offered by Point of Presence Table B.4.1.4.

B.1.2.17.2 Government-Maintained Tables

Instruction Tables accompany the price tables throughout Section B and define the CLIN structures and charging mechanisms for the CLINs. In these tables, each CLIN is given a description of the service it provides and is assigned a billing frequency and a charging unit. The Notes column indicates if the CLIN is ICB, NSP or optional. CLINs are mandatory unless identified as optional in the Notes column. When multiple CLINs occupy the same row of an instruction table (e.g., NRC and MRC CLINs, or NRC, MRC and Usage CLINs):

- If a single charging unit is listed, it applies to all CLINs in that row.
- If the CLINs in that row do not share a common charging unit, the charging units will be listed separately and separated by semicolons.
- The information in the Notes column applies to all CLINs in that row unless stated otherwise.

Reference Tables contain information that is the same for all contractors. The government will maintain each reference table for contractors to access via GSA Systems. Examples include Country/Jurisdiction Identifications Table B.4.2.1 and Network Site Codes Table B.4.1.8.

[5] In SRE Catalog Prices Table B.2.10.3.2, the value “-1” in the Task Order Number column indicates a catalog price that is valid for all task orders.

B.1.3 Catalog Pricing Requirements - General

For certain EIS services, contractors must develop and maintain catalog-style offerings as part of the pricing requirements. Following are the services for which catalog requirements exist, along with the section references where they are found:

- Cloud Service – Section B.2.5
- Wireless Service – Section B.2.6
- Commercial Mobile Satellite Service – Section B.2.7.1
- Managed Security Service – Section B.2.8.5
- Service Related Equipment – Section B.2.10

For each service that requires a catalog pricing approach as part of the overall service pricing, the contractor shall develop and maintain an online catalog that meets the general requirements specified in this section, and also the service-specific requirements found in the section associated with the service.

B.1.3.1 Requirements for Catalog Pricing Information

Prices for catalog items shall be based on a discount from the Official List Price (OLP). OLP is a common term defined under EIS to include a variety of possible list price types or trade names. For example, if the catalog item is equipment not manufactured by the contractor, the OLP could be called, “Original Equipment Manufacturer’s Published List Price.” When the catalog item is a service provided by the contractor, the OLP could be called the contractor’s “Published List Price” for the service. Many other trade names may exist to identify the price to be associated with the OLP for a particular catalog item. The contractor shall provide the OLP trade name(s) that are associated with its catalog item OLPs for each catalog offering. Other specific pricing requirements, discount strategies and catalog elements unique to the catalog items are further defined in the service sections.

All pricing catalogs provided by the contractor shall contain, at a minimum, the data elements defined in the appropriate catalog pricing section and in Section B.1.2.14.

The contractor may organize its catalogs as it sees fit, subject to the following requirements:

- Catalog content and pricing shall be accessible by authorized users at any time (i.e., 24x7x365).

- Catalog content shall be organized logically, with features that enable common online browsing functions such as search and comparison.
- The online catalog shall meet the Section 508 requirements in Section C.4.
- The appropriate item identification shall be provided in the catalog to identify the catalog items being ordered (see individual sections for specific requirements).
- Contract prices and price-related information shall be provided to users who access the catalog (TO-specific prices need not be included).
- The contractor shall supply sufficient information to allow the government to verify the OLP and the accuracy of the item description in terms of capabilities and limitations, or other distinguishing characteristics, such as color, or other cosmetic features that could affect the price.
- All prices in catalogs shall be provided in U.S. dollars.
- Contract discounts offered shall not vary by geographic location. Additional discounts may be offered on TOs.
- Each catalog item shall belong to only a single discount class.
- Percentage discounts in class discount tables shall be specified as decimal values between 0 and 1, inclusive.
- The contractor shall keep catalog information up to date including, but not limited to, the OLP.
- If the OLP for a particular catalog item is not available, the price charged shall be agreed upon between the government and the ordering agency at the time of TO award. The contractor shall populate the OLP column with the agreed-upon price, populate the No List Price column with “T”, and specify a discount class that has a discount of zero.
- Price elements other than OLP shall be provided as appropriate and available.
- Additional information may be provided by the contractor in its catalog at its option.

B.1.3.2 Catalog Operational Rules

The following operational conditions, or rules, shall apply to the contractor’s catalog for the term of the contract:

- The contractor shall be solely responsible for developing and maintaining its online catalog in accordance with the provisions of this contract.

- The catalog shall be accessible via the Internet under the access controls provided by the contractor.
- Authorized personnel shall be allowed access to the catalog at the direction of either the government or the contractor.
- For catalog-based services and equipment, only items listed in the contractor's current catalog may be ordered.
- The catalog as provided at any given point in time during the term of the contract shall constitute the contractor's official source of contract prices for items in the catalog.
- The contractor may change its catalog at any time at its option as follows:
    - An item shall be added by providing at least the minimum data elements required for that item as defined in each service section.
    - Discount classes for items shall only be added, removed, or changed via contract modification, except that TO-specific discount increases are permitted for any discount class at any time using the TO submission process (see Section J.4.1 for details).
    - Items and their associated data elements may be changed at any time, except for end-of-life items. Catalog item prices shall not be increased unless the increased price results from an increase in the OLP. Discounts shall not be decreased for items with a discount structure.
    - The contractor shall ensure that the OLP is current and shall only change the value in the OLP column for that purpose.
    - Where appropriate, items may be removed by being designated as end-of-life; users shall have the option of masking or viewing end-of-life items when viewing the catalog.
    - End-of-life items shall not be changed once designated as end-of-life.
    - All changes to the catalog shall be conveyed to the government as defined in Section J.4.2.

B.1.3.3 Termination of Support

If the contractor desires to discontinue support for an item (for example, an item that will no longer be supported by the manufacturer), the contractor shall notify the GSA CO and any affected agencies at least 18 months before support is stopped (see Section B.2.10.7 for an exception for mobile devices). As appropriate, at time of notification, the contractor shall also recommend a solution acceptable to the government that ensures service continuity. The contractor shall continue to provide support for the existing item at the established price until a solution acceptable to the government is implemented by

the contractor. Following notification of the GSA CO and affected agencies, the contractor shall no longer accept orders for the item.

B.2 Pricing Tables

B.2.1 Data Service

B.2.1.1 Virtual Private Network Service

The technical requirements for Virtual Private Network Service (VPNS) are defined in Section C.2.1.1.

B.2.1.1.1 VPNS Price Structure

The price structure for VPNS includes the following elements:

1. Transport Charges
2. (Optional) Transport with Embedded Access Charges
3. Feature Charges

The pricing associated with a VPNS is dependent upon a number of factors, including the number of sites, bandwidth requirements, additional security services, and the type of access. Network design and engineering services can be provided using Service Related Labor CLINs as provided in Section B.2.11. SRE pricing for the user-to-network interfaces shall be provided in accordance with Section B.2.10.

B.2.1.1.2 VPNS Access

Pricing for access arrangements is described in Section B.2.9. Access includes wireline, Ethernet, wireless, and satellite. Remote VPNS access (e.g., DSL, Cable) shall be ordered via a TUC.

As an option, specific shared Ethernet and Satellite access speeds may be acquired as embedded with the port for a combined price.

For embedded access, the speed of the access component shall equal or exceed the speed of the port with which it is embedded.

Table B.2.1.1.3.3 provides the pricing instructions for embedded access.

B.2.1.1.3 VPNS Transport

All configurations of Quality of Service (QoS) are defined in Section C.2.1.1.1.4. Capabilities #7, #8, and #9 shall be included in the port price (i.e., NSP). Since QoS is also ICB, a case number shall be assigned for each port purchase and a description shall be provided of how the port will be configured.

All network security services are defined in Section C.2.1.1.1.4. Capabilities #2, #3, and #4 shall be included in the port price (i.e., NSP).

Table B.2.1.1.3.1 provides the format for pricing VPNS ports, ports with embedded access, and QoS. Tables B.2.1.1.3.2, B.2.1.1.3.3 and B.2.1.1.3.4 provide the pricing instructions.

B.2.1.1.3.1 VPNS Port Prices Table

CLIN	Case Number*	Task Order Number	Country/ Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Case Number applies to ICB CLINs only
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.1.1.3.2 VPNS Port Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
VN00001	MRC	T1	Port	
VN00002	MRC	T3	Port	
VN00003	MRC	Ethernet – 1 Mbps	Port	
VN00004	MRC	Ethernet – 3 Mbps	Port	
VN00005	MRC	Ethernet – 6 Mbps	Port	
VN00006	MRC	Ethernet – 10 Mbps	Port	
VN00007	MRC	Ethernet – 20 Mbps	Port	
VN00008	MRC	Ethernet – 30 Mbps	Port	
VN00009	MRC	Ethernet – 40 Mbps	Port	
VN00010	MRC	Ethernet – 50 Mbps	Port	
VN00011	MRC	Ethernet – 60 Mbps	Port	

CLIN	Frequency	Description	Charging Unit	Notes
VN00012	MRC	Ethernet – 70 Mbps	Port	
VN00013	MRC	Ethernet – 80 Mbps	Port	
VN00014	MRC	Ethernet – 90 Mbps	Port	
VN00015	MRC	Ethernet – 100 Mbps	Port	
VN00016	MRC	Ethernet – 200 Mbps	Port	
VN00017	MRC	Ethernet – 300 Mbps	Port	
VN00018	MRC	Ethernet – 400 Mbps	Port	
VN00019	MRC	Ethernet – 500 Mbps	Port	
VN00020	MRC	Ethernet – 600 Mbps	Port	
VN00021	MRC	Ethernet – 700 Mbps	Port	
VN00022	MRC	Ethernet – 800 Mbps	Port	
VN00023	MRC	Ethernet – 900 Mbps	Port	
VN00024	MRC	Ethernet – 1 Gbps	Port	
VN00025	MRC	Ethernet – 2 Gbps	Port	
VN00026	MRC	Ethernet – 3 Gbps	Port	
VN00027	MRC	Ethernet – 10 Gbps	Port	
VN00028	MRC	OC-3c	Port	
VN00029	MRC	OC-12c	Port	
VN00030	MRC	OC-48c	Port	
VN00031	MRC	OC-192c	Port	
VN00032	MRC	OC-768c	Port	Optional

CLIN	Frequency	Description	Charging Unit	Notes
VN00033	MRC	E1	Port	Optional. Non-domestic only
VN00034	MRC	E3	Port	Optional. Non-domestic only
VN00035	MRC	ISDN, 64 Kbps	Port	Optional
VN00036	MRC	ISDN, 128 Kbps	Port	Optional
VN00037	MRC	ISDN, 64 Kbps, backup	Port	Optional
VN00038	MRC	ISDN, 128 Kbps, backup	Port	Optional
VN20001	MRC	Ethernet – 3 Mbps committed, scalable to 10 Mbps	Port	Optional
VN20002	MRC	Ethernet – 6 Mbps committed, scalable to 10 Mbps	Port	Optional
VN20003	MRC	Ethernet – 20 Mbps committed, scalable to 100 Mbps	Port	Optional
VN20004	MRC	Ethernet – 30 Mbps committed, scalable to 100 Mbps	Port	Optional
VN20005	MRC	Ethernet – 50 Mbps committed, scalable to 100 Mbps	Port	Optional
VN20006	MRC	Ethernet – 200 Mbps committed, scalable to 1 Gbps	Port	Optional
VN20007	MRC	Ethernet – 300 Mbps committed, scalable to 1 Gbps	Port	Optional
VN20008	MRC	Ethernet – 2 Gbps committed, scalable to 10 Gbps	Port	Optional
VN20009	MRC	Ethernet – 3 Gbps committed, scalable to 10 Gbps	Port	Optional
VN21001	Usage	Ethernet Bandwidth-on-Demand temporary bandwidth increase of 1 Mbps per day; 1 Mbps ≤ committed bandwidth < 10 Mbps	Mbps per day	Optional. Requires scalable Ethernet port
VN21002	Usage	Ethernet Bandwidth-on-Demand temporary bandwidth increase of 10 Mbps per day; 10 Mbps ≤ committed bandwidth < 100 Mbps	10 Mbps per day	Optional. Requires scalable Ethernet port

CLIN	Frequency	Description	Charging Unit	Notes
VN21003	Usage	Ethernet Bandwidth-on-Demand temporary bandwidth increase of 100 Mbps per day; 100 Mbps ≤ committed bandwidth < 1 Gbps	100 Mbps per day	Optional. Requires scalable Ethernet port
VN21004	Usage	Ethernet Bandwidth-on-Demand temporary bandwidth increase of 1 Gbps per day; 1 Gbps ≤ committed bandwidth < 10 Gbps	Gbps per day	Optional. Requires scalable Ethernet port
VN30001	MRC	T3 burstable – 5 Mbps committed	Port	
VN30002	MRC	T3 burstable – 10 Mbps committed	Port	
VN30003	MRC	T3 burstable – 15 Mbps committed	Port	
VN30004	MRC	T3 burstable – 20 Mbps committed	Port	
VN30005	MRC	T3 burstable – 30 Mbps committed	Port	
VN30009	Usage	T3 burstable overage	Mbps	
VN30010	MRC	Ethernet – 20 Mbps committed, burstable to 100 Mbps	Port	
VN30011	MRC	Ethernet – 30 Mbps committed, burstable to 100 Mbps	Port	
VN30012	MRC	Ethernet – 40 Mbps committed, burstable to 100 Mbps	Port	
VN30013	MRC	Ethernet – 50 Mbps committed, burstable to 100 Mbps	Port	
VN30021	MRC	Ethernet – 200 Mbps committed, burstable to 1 Gbps	Port	
VN30022	MRC	Ethernet – 300 Mbps committed, burstable to 1 Gbps	Port	
VN30023	MRC	Ethernet – 400 Mbps committed, burstable to 1 Gbps	Port	
VN30024	MRC	Ethernet – 500 Mbps committed, burstable to 1 Gbps	Port	
VN30025	MRC	Ethernet – 600 Mbps committed, burstable to 1 Gbps	Port	
VN31020	Usage	Ethernet burstable overage for 20 Mbps committed port burstable to 100 Mbps	Mbps	
VN31030	Usage	Ethernet burstable overage for 30 Mbps committed port burstable to 100 Mbps	Mbps	

CLIN	Frequency	Description	Charging Unit	Notes
VN31040	Usage	Ethernet burstable overage for 40 Mbps committed port burstable to 100 Mbps	Mbps	
VN31050	Usage	Ethernet burstable overage for 50 Mbps committed port burstable to 100 Mbps	Mbps	
VN31200	Usage	Ethernet burstable overage for 200 Mbps committed port burstable to 1 Gbps	Mbps	
VN31300	Usage	Ethernet burstable overage for 300 Mbps committed port burstable to 1 Gbps	Mbps	
VN31400	Usage	Ethernet burstable overage for 400 Mbps committed port burstable to 1 Gbps	Mbps	
VN31500	Usage	Ethernet burstable overage for 500 Mbps committed port burstable to 1 Gbps	Mbps	
VN31600	Usage	Ethernet burstable overage for 600 Mbps committed port burstable to 1 Gbps	Mbps	
VN40001	NRC	Expedited provisioning within 24 hours	Port	

Because agencies have differing interests for balancing budgetary control against ordering complexity, Table B.2.1.1.3.2 includes two mandatory pricing mechanisms for achieving dynamic bandwidth: scalable bandwidth and burstable bandwidth.

Scalable bandwidth is ordered in anticipation of a future, temporary need for increased capacity. A scalable Ethernet transport MRC CLIN shall guarantee a committed bandwidth while ensuring the availability of the increased capacity. An Ethernet Bandwidth-on-Demand usage CLIN shall provide the increased capacity and must be ordered for the period of time during which the increased capacity will be required. An example of a valid CLIN pairing is Ethernet Bandwidth-on-Demand CLIN VN21002 used with scalable Ethernet transport CLIN VN20004.

Burstable bandwidth allows an agency to subscribe to a bandwidth commitment that is less than the full bandwidth of the selected VPNS port, but may burst to the full bandwidth of the selected port. The bandwidth commitment equals the portion capacity of a circuit (as measured in bandwidth) that an agency may use in a monthly period without incurring an overage charge. A T3 burstable or Ethernet burstable CLIN shall guarantee a committed bandwidth while ensuring the availability of the increased capacity.

Bandwidth used in excess of the committed burstable bandwidth shall be invoiced via an overage usage CLIN. For each T3 burstable or Ethernet

burstable MRC CLIN, a corresponding burstable overage usage CLIN shall be auto-sold to simplify ordering. For example, Ethernet burstable overage CLIN VN31500 shall be auto-sold with Ethernet burstable transport CLIN VN30024, and T3 burstable overage CLIN VN30009 shall be auto-sold with T3 burstable CLIN VN30003.

With burstable bandwidth, agencies shall only be charged for the amount of bandwidth used on a sustained level (95th percentile). Bandwidth shall be measured (or sampled) from the switch or router every 5 minutes. At the end of the month, the top 5% of data shall be discarded. The next highest measurement shall determine the billable usage for the month. Overages shall be billed in one-megabit per second increments for usage above the selected bandwidth commitment.

Table B.2.1.1.3.2 includes an expedited provisioning CLIN that shall be used to provision, within 24 hours rather than the standard provisioning period, a VPNS port CLIN at a higher bandwidth, subject to the restrictions below. This 24-hour provisioning shall be accomplished by ordering the expedited provisioning CLIN concurrent with the new, higher bandwidth port CLIN. The expedited provisioning CLIN shall only be used when moving from one bandwidth to another, where sufficient physical access capacity exists and where either:

1. The existing port is T3 burstable, and the new port does not exceed T3, or
2. The existing port is Ethernet, and the new port does not exceed the physical capacity of the existing port.

B.2.1.1.3.3 VPNS Port with Embedded Access Pricing Instructions Table

MRC CLIN	Description	Charging Unit	Notes
VN01001	Embedded Satellite – 1.54 Mbps	Port	Optional
VN01002	Embedded Satellite ~~Access~~ – 12 Mbps	Port	Optional
VN01003	Embedded T1	Port	Optional
VN01004	Embedded T3	Port	Optional
VN01005	Embedded Shared Ethernet – 1 Mbps	Port	Optional
VN01006	Embedded Shared Ethernet – 10 Mbps	Port	Optional

MRC CLIN	Description	Charging Unit	Notes
VN01007	Embedded Shared Ethernet – 50 Mbps	Port	Optional
VN01008	Embedded Shared Ethernet – 100 Mbps	Port	Optional
VN01009	Embedded Shared Ethernet – 700 Mbps	Port	Optional
VN01010	Embedded Shared Ethernet – 1 Gbps	Port	Optional
VN01011	Embedded Shared Ethernet – 3 Gbps	Port	Optional

B.2.1.1.3.4 VPNS Quality of Service (QoS)

VPNS QoS applies to the services in Tables B.2.1.1.3.2 and B.2.1.1.3.3.

MRC CLIN	Description	Charging Unit	Notes
VN10000	Quality of Service (QoS)	Port	ICB, NSP

B.2.1.1.4 VPNS Features

Table B.2.1.1.4.1 provides the format for pricing VPNS features. Table B.2.1.1.4.2 provides the pricing instructions for the features supported by VPNS. The requirement in Section C.2.1.1.2, ID Number 1, high availability options, shall be priced using CLINs from other sections such as B.2.9 (e.g., access diversity) and B.2.10 (e.g., a redundant router) or a TUC.

B.2.1.1.4.1 VPNS Feature Prices Table

CLIN*	Case Number**	Task Order Number	Country/Jurisdiction ID***	Price	Price Start Date	Price Stop Date

* See feature pricing instructions in Table B.2.1.1.4.2 for the applicable charging mechanisms and charging units for each feature
** Applies to ICB CLINs only
*** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.1.1.4.2 VPNS Feature Pricing Instructions Table*

MRC CLIN	Description	Charging Unit	Notes
VN90002	Interworking Services	Port	Optional

* See Section C.2.1.1.2 for details

B.2.1.1.5 VPNS Task Order Unique CLINs

Table B.2.1.1.5.1 provides the format for pricing TUCs supported by VPNS. Table B.2.1.1.5.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.1.1.5.1 VPNS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.1.1.5.2 VPNS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
VN99990	VN99991	VN99992	VPNS Task Order Unique	ICB	ICB

B.2.1.2 Ethernet Transport Service

The technical requirements for Ethernet Transport Service (ETS) are defined in Section C.2.1.2. Access arrangements to connect to the contractor's ETS network shall be provided in accordance with Section B.2.9.

B.2.1.2.1 Ethernet Transport Service Price Structure

ETS pricing includes the following elements:

1. Port price
2. Ethernet Virtual Connection (EVC) price (E-LINE only)
3. Features

E-LINE service requires the provisioning of two ports (point-to-point) and an EVC connecting them; the total price shall be the sum of the prices of the two ports, the connecting EVC, and any selected features.

E-LAN service requires the provisioning of two or more ports; the total price shall be the sum of the prices of the ports (which may not be the same speed) and any selected features.

All configurations of Quality of Service (QoS) are defined in Section C.2.1.2.1.4. Capability #26 shall be included in the port price (i.e., NSP). Since QoS is also ICB, a case number shall be assigned for each port purchase and a description shall be provided of how the port will be configured.

B.2.1.2.2 E-LINE Port Pricing

Table B.2.1.2.2.1 provides the format for pricing information for E-LINE port prices. Table B.2.1.2.2.2 provides the appropriate CLINs.

B.2.1.2.2.1 E-LINE Port Prices Table

CLIN	Case Number*	Task Order Number	Country/Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.1.2.2.2 E-LINE Port Pricing Instructions Table

MRC CLIN	Description	Charging Unit	Notes
EN00001	E-LINE Ethernet Network Interface – 10 Mbps	Port	
EN00002	E-LINE Ethernet Network Interface – 100 Mbps	Port	
EN00003	E-LINE Ethernet Network Interface – 1 Gbps	Port	
EN00004	E-LINE Ethernet Network Interface – 10 Gbps	Port	
EN00005	E-LINE Ethernet Network Interface – 40 Gbps	Port	Optional
EN00006	E-LINE Ethernet Network Interface Quality of Service (QoS)	Port	NSP, ICB

B.2.1.2.3 E-LINE EVC Pricing

Table B.2.1.2.3.1 provides the format for E-LINE point-to-point EVCs. Pricing is in terms of committed information rate (CIR). CLINs are provided in Table B.2.1.2.3.2.

B.2.1.2.3.1 E-LINE EVC Prices Table

CLIN	Case Number*	Task Order Number	Originating Country/ Jurisdiction ID**	Terminating Country/ Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.1.2.3.2 E-LINE EVC Pricing Instructions Table

MRC CLIN	Description	Charging Unit	Notes
EN00010	E-LINE EVC - 1 Mbps (point-to-point)	EVC	
EN00011	E-LINE EVC - 2 Mbps (point-to-point)	EVC	
EN00012	E-LINE EVC - 3 Mbps (point-to-point)	EVC	
EN00013	E-LINE EVC - 4 Mbps (point-to-point)	EVC	
EN00014	E-LINE EVC - 5 Mbps (point-to-point)	EVC	
EN00015	E-LINE EVC - 6 Mbps (point-to-point)	EVC	
EN00016	E-LINE EVC - 7 Mbps (point-to-point)	EVC	
EN00017	E-LINE EVC - 8 Mbps (point-to-point)	EVC	
EN00018	E-LINE EVC - 9 Mbps (point-to-point)	EVC	
EN00019	E-LINE EVC - 10 Mbps (point-to-point)	EVC	
EN00020	E-LINE EVC - 20 Mbps (point-to-point)	EVC	
EN00021	E-LINE EVC - 30 Mbps (point-to-point)	EVC	
EN00022	E-LINE EVC - 40 Mbps (point-to-point)	EVC	
EN00023	E-LINE EVC - 50 Mbps (point-to-point)	EVC	
EN00024	E-LINE EVC - 60 Mbps (point-to-point)	EVC	
EN00025	E-LINE EVC - 70 Mbps (point-to-point)	EVC	
EN00026	E-LINE EVC - 80 Mbps (point-to-point)	EVC	
EN00027	E-LINE EVC - 90 Mbps (point-to-point)	EVC	
EN00028	E-LINE EVC - 100 Mbps (point-to-point)	EVC	
EN00029	E-LINE EVC - 200 Mbps (point-to-point)	EVC	
EN00030	E-LINE EVC - 300 Mbps (point-to-point)	EVC	
EN00031	E-LINE EVC - 400 Mbps (point-to-point)	EVC	
EN00032	E-LINE EVC - 500 Mbps (point-to-point)	EVC	
EN00033	E-LINE EVC - 600 Mbps (point-to-point)	EVC	
EN00034	E-LINE EVC - 700 Mbps (point-to-point)	EVC	

MRC CLIN	Description	Charging Unit	Notes
EN00035	E-LINE EVC - 800 Mbps (point-to-point)	EVC	
EN00036	E-LINE EVC - 900 Mbps (point-to-point)	EVC	
EN00037	E-LINE EVC - 1 Gbps (point-to-point)	EVC	
EN00038	E-LINE EVC - 2 Gbps (point-to-point)	EVC	
EN00039	E-LINE EVC - 3 Gbps (point-to-point)	EVC	
EN00040	E-LINE EVC - 4 Gbps (point-to-point)	EVC	
EN00041	E-LINE EVC - 5 Gbps (point-to-point)	EVC	
EN00042	E-LINE EVC - 6 Gbps (point-to-point)	EVC	
EN00043	E-LINE EVC - 7 Gbps (point-to-point)	EVC	
EN00044	E-LINE EVC - 8 Gbps (point-to-point)	EVC	
EN00045	E-LINE EVC - 9 Gbps (point-to-point)	EVC	
EN00046	E-LINE EVC - 10 Gbps (point-to-point)	EVC	
EN00047	E-LINE EVC - 20 Gbps (point-to-point)	EVC	Optional
EN00048	E-LINE EVC - 30 Gbps (point-to-point)	EVC	Optional
EN00049	E-LINE EVC - 40 Gbps (point-to-point)	EVC	Optional

B.2.1.2.4 E-LAN Port Pricing

Table B.2.1.2.4.1 provides the format for pricing information for E-LAN port prices. Table B.2.1.2.4.2 provides the CLINs.

B.2.1.2.4.1 E-LAN Port Prices Table

CLIN	Case Number*	Task Order Number	Country/Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.1.2.4.2 E-LAN Port Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
EN00501	MRC	E-LAN Ethernet – 1 Mbps	Port	
EN00502	MRC	E-LAN Ethernet – 2 Mbps	Port	
EN00503	MRC	E-LAN Ethernet – 3 Mbps	Port	

CLIN	Frequency	Description	Charging Unit	Notes
EN00504	MRC	E-LAN Ethernet – 4 Mbps	Port	
EN00505	MRC	E-LAN Ethernet – 5 Mbps	Port	
EN00506	MRC	E-LAN Ethernet – 6 Mbps	Port	
EN00507	MRC	E-LAN Ethernet – 7 Mbps	Port	
EN00508	MRC	E-LAN Ethernet – 8 Mbps	Port	
EN00509	MRC	E-LAN Ethernet – 9 Mbps	Port	
EN00510	MRC	E-LAN Ethernet – 10 Mbps	Port	
EN00520	MRC	E-LAN Ethernet – 20 Mbps	Port	
EN00530	MRC	E-LAN Ethernet – 30 Mbps	Port	
EN00540	MRC	E-LAN Ethernet – 40 Mbps	Port	
EN00550	MRC	E-LAN Ethernet – 50 Mbps	Port	
EN00560	MRC	E-LAN Ethernet – 60 Mbps	Port	
EN00570	MRC	E-LAN Ethernet – 70 Mbps	Port	
EN00580	MRC	E-LAN Ethernet – 80 Mbps	Port	
EN00590	MRC	E-LAN Ethernet – 90 Mbps	Port	
EN00600	MRC	E-LAN Ethernet – 100 Mbps	Port	
EN00620	MRC	E-LAN Ethernet – 200 Mbps	Port	
EN00630	MRC	E-LAN Ethernet – 300 Mbps	Port	
EN00640	MRC	E-LAN Ethernet – 400 Mbps	Port	
EN00650	MRC	E-LAN Ethernet – 500 Mbps	Port	
EN00660	MRC	E-LAN Ethernet – 600 Mbps	Port	

CLIN	Frequency	Description	Charging Unit	Notes
EN00670	MRC	E-LAN Ethernet – 700 Mbps	Port	
EN00680	MRC	E-LAN Ethernet – 800 Mbps	Port	
EN00690	MRC	E-LAN Ethernet – 900 Mbps	Port	
EN00700	MRC	E-LAN Ethernet – 1 Gbps	Port	
EN00720	MRC	E-LAN Ethernet – 2 Gbps	Port	
EN00730	MRC	E-LAN Ethernet – 3 Gbps	Port	
EN00740	MRC	E-LAN Ethernet – 4 Gbps	Port	
EN00750	MRC	E-LAN Ethernet – 5 Gbps	Port	
EN00760	MRC	E-LAN Ethernet – 6 Gbps	Port	
EN00770	MRC	E-LAN Ethernet – 7 Gbps	Port	
EN00780	MRC	E-LAN Ethernet – 8 Gbps	Port	
EN00790	MRC	E-LAN Ethernet – 9 Gbps	Port	
EN00800	MRC	E-LAN Ethernet – 10 Gbps	Port	
EN00850	MRC	E-LAN Ethernet – 20 Gbps	Port	Optional
EN00900	MRC	E-LAN Ethernet – 30 Gbps	Port	Optional
EN01000	MRC	E-LAN Ethernet – 40 Gbps	Port	Optional
EN20001	MRC	E-LAN Ethernet – 3 Mbps committed, scalable to 10 Mbps	Port	
EN20002	MRC	E-LAN Ethernet – 6 Mbps committed, scalable to 10 Mbps	Port	
EN20003	MRC	E-LAN Ethernet – 20 Mbps committed, scalable to 100 Mbps	Port	
EN20004	MRC	E-LAN Ethernet – 30 Mbps committed, scalable to 100 Mbps	Port	

CLIN	Frequency	Description	Charging Unit	Notes
EN20005	MRC	E-LAN Ethernet – 50 Mbps committed, scalable to 100 Mbps	Port	
EN20006	MRC	E-LAN Ethernet – 200 Mbps committed, scalable to 1 Gbps	Port	
EN20007	MRC	E-LAN Ethernet – 300 Mbps committed, scalable to 1 Gbps	Port	
EN20008	MRC	E-LAN Ethernet – 2 Gbps committed, scalable to 10 Gbps	Port	
EN20009	MRC	E-LAN Ethernet – 3 Gbps committed, scalable to 10 Gbps	Port	
EN21001	Usage	E-LAN Ethernet Bandwidth-on-Demand temporary bandwidth increase of 1 Mbps per day; 1 Mbps ≤ committed bandwidth < 10 Mbps	Mbps per day	Requires scalable E-LAN Ethernet port
EN21002	Usage	E-LAN Ethernet Bandwidth-on-Demand temporary bandwidth increase of 10 Mbps per day; 10 Mbps ≤ committed bandwidth < 100 Mbps	10 Mbps per day	Requires scalable E-LAN Ethernet port
EN21003	Usage	E-LAN Ethernet Bandwidth-on-Demand temporary bandwidth increase of 100 Mbps per day; 100 Mbps ≤ committed bandwidth < 1 Gbps	100 Mbps per day	Requires scalable E-LAN Ethernet port
EN21004	Usage	E-LAN Ethernet Bandwidth-on-Demand temporary bandwidth increase of 1 Gbps per day; 1 Gbps ≤ committed bandwidth < 10 Gbps	Gbps per day	Requires scalable E-LAN Ethernet port
EN30010	MRC	E-LAN Ethernet – 20 Mbps committed, burstable to 100 Mbps	Port	
EN30011	MRC	E-LAN Ethernet – 30 Mbps committed, burstable to 100 Mbps	Port	
EN30012	MRC	E-LAN Ethernet – 40 Mbps committed, burstable to 100 Mbps	Port	
EN30013	MRC	E-LAN Ethernet – 50 Mbps committed, burstable to 100 Mbps	Port	
EN30014	MRC	E-LAN Ethernet – 200 Mbps committed, burstable to 1 Gbps	Port	
EN30015	MRC	E-LAN Ethernet – 300 Mbps committed, burstable to 1 Gbps	Port	
EN30016	MRC	E-LAN Ethernet – 400 Mbps committed, burstable to 1 Gbps	Port	

CLIN	Frequency	Description	Charging Unit	Notes
EN30017	MRC	E-LAN Ethernet – 500 Mbps committed, burstable to 1 Gbps	Port	
EN30018	MRC	E-LAN Ethernet – 600 Mbps committed, burstable to 1 Gbps	Port	
EN31020	Usage	E-LAN Ethernet burstable overage for 20 Mbps committed port burstable to 100 Mbps	Mbps	
EN31030	Usage	E-LAN Ethernet burstable overage for 30 Mbps committed port burstable to 100 Mbps	Mbps	
EN31040	Usage	E-LAN Ethernet burstable overage for 40 Mbps committed port burstable to 100 Mbps	Mbps	
EN31050	Usage	E-LAN Ethernet burstable overage for 50 Mbps committed port burstable to 100 Mbps	Mbps	
EN31200	Usage	E-LAN Ethernet burstable overage for 200 Mbps committed port burstable to 1 Gbps	Mbps	
EN31300	Usage	E-LAN Ethernet burstable overage for 300 Mbps committed port burstable to 1 Gbps	Mbps	
EN31400	Usage	E-LAN Ethernet burstable overage for 400 Mbps committed port burstable to 1 Gbps	Mbps	
EN31500	Usage	E-LAN Ethernet burstable overage for 500 Mbps committed port burstable to 1 Gbps	Mbps	
EN31600	Usage	E-LAN Ethernet burstable overage for 600 Mbps committed port burstable to 1 Gbps	Mbps	
EN40001	NRC	E-LAN Expedited provisioning within 24 hours	Port	
EN50001	MRC	E-LAN Quality of Service (QoS)	Port	NSP, ICB

Because agencies have differing interests for balancing budgetary control against ordering complexity, Table B.2.1.2.4.2 includes two mandatory pricing mechanisms for achieving dynamic bandwidth: scalable bandwidth and burstable bandwidth.

> **Scalable bandwidth** is ordered in anticipation of a future, temporary need for increased capacity. A scalable E-LAN transport MRC CLIN shall guarantee a committed bandwidth while ensuring the availability of the increased capacity. An E-LAN Bandwidth-on-Demand usage CLIN shall provide the increased capacity and must be ordered for the period of time during which the increased capacity will be required. An example of a valid CLIN pairing is E-LAN Ethernet

Bandwidth-on-Demand CLIN EN21002 used with scalable E-LAN Ethernet transport CLIN EN20004.

Burstable bandwidth allows an agency to subscribe to a bandwidth commitment that is less than the full bandwidth of the selected E-LAN Ethernet port, but may burst to the full bandwidth of the selected port. The bandwidth commitment equals the portion capacity of a circuit (as measured in bandwidth) that an agency may use in a monthly period without incurring an overage charge. An E-LAN Ethernet burstable CLIN shall guarantee a committed bandwidth while ensuring the availability of the increased capacity.

Bandwidth used in excess of the committed burstable bandwidth shall be invoiced via an overage usage CLIN. For each E-LAN Ethernet burstable MRC CLIN, a corresponding burstable overage usage CLIN shall be auto-sold to simplify ordering. For example, E-LAN Ethernet burstable overage CLIN EN31500 shall be auto-sold with Ethernet burstable transport CLIN EN30017.

With burstable bandwidth, agencies shall only be charged for the amount of bandwidth used on a sustained level (95th percentile). Bandwidth shall be measured (or sampled) from the switch or router every 5 minutes. At the end of the month, the top 5% of data shall be discarded. The next highest measurement shall determine the billable usage for the month. Overages shall be billed in one-megabit per second increments for usage above the selected bandwidth commitment.

Table B.2.1.2.4.2 includes an expedited provisioning CLIN that shall be used to provision, within 24 hours rather than the standard provisioning period, an E-LAN Ethernet port CLIN at a higher bandwidth. This 24-hour provisioning shall be accomplished by ordering the expedited provisioning CLIN concurrent with the new, higher bandwidth port CLIN. The expedited provisioning CLIN shall only be used when moving from one bandwidth to another where sufficient physical access capacity exists and the new port does not exceed the physical capacity of the existing port.

B.2.1.2.5 Ethernet Transport Features Pricing

Table B.2.1.2.5.1 provides the formats for pricing Ethernet features.

B.2.1.2.5.1 Ethernet Transport Feature Prices Table (Reserved for future use)

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.1.2.6 Ethernet Transport Task Order Unique CLINs

Table B.2.1.2.6.1 provides the format for pricing TUCs supported by Ethernet. Table B.2.1.2.6.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.1.2.6.1 Ethernet Transport TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.1.2.6.2 Ethernet Transport TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
EN99990	EN99991	EN99992	ETS Task Order Unique	ICB	ICB

B.2.1.3 Optical Wavelength Service

The technical requirements for Optical Wavelength Service (OWS) are defined in Section C.2.1.3. OWS shall be provided over Wavelength Division Multiplexing (WDM).

B.2.1.3.1 OWS Price Structure

The price structure for OWS includes the following elements:

1. MRC per wavelength for transport
2. Feature Charges

Where access is used to connect the SDP to the contractor's designated connecting POP, access prices shall be provided in accordance with Section B.2.9. Prices for any associated SRE shall be provided in accordance with Section B.2.10.

B.2.1.3.2 OWS Transport

The MRC for CONUS-to-CONUS transport consists of a fixed component that is determined based on mileage band. CONUS-to-CONUS distance shall be based on the total mileage between the contractor's designated connecting POPs for any two customer locations. CONUS-to-CONUS distances shall be calculated using the distance formula listed in Section B.1.2.7. The MRC for OCONUS and non-domestic consists of a fixed component plus a distance dependent (per mile) formula. Distance involving

OCONUS or non-domestic locations shall be calculated using the shortest airline miles obtained from the haversine great-circle distance formula shown below:

$$a = \sin^2(\Delta\varphi/2) + \cos\varphi 1 \cdot \cos\varphi 2 \cdot \sin^2(\Delta\lambda/2)$$

$$c = 2 \cdot \text{atan2}(\sqrt{a}, \sqrt{(1-a)})$$

$$\text{distance} = R \cdot c$$

where φ is latitude, λ is longitude, R is earth's radius (mean radius = 6,371km).

Table B.2.1.3.2.1 provides the formats for the pricing information for Metro OWS. The contractor shall provide a single price for Metro OWS (i.e., transport in a domestic metropolitan area). Thus, the Metro OWS price shall not vary by metropolitan area. The contractor shall list the Network Site Code (NSC) for each location where Metro OWS is provided as defined in Section B.4.1.12.

Table B.2.1.3.2.2 provides the formats for the pricing information for CONUS OWS. Table B.2.1.3.2.3 provides the formats for the pricing information for OCONUS OWS. Table B.2.1.3.2.4 provides the formats for the pricing information for non-domestic OWS. The contractor shall also list the mileage bands for the appropriate transport charges in Tables B.2.1.3.2.2, B.2.1.3.2.3, and B.2.1.3.2.4.

Table B.2.1.3.2.5 provides the wavelength speeds and applicable charging units for OWS on the WDM.

Finally, the contractor shall list the originating and terminating Country/Jurisdiction IDs for OWS transport in Tables B.2.1.3.2.3 and B.2.1.3.2.4. The Country/Jurisdiction IDs are listed in Table B.4.2.1.

B.2.1.3.2.1 Metro OWS Transport Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.1.3.2.2 CONUS OWS Transport Prices Table

CLIN	Case Number*	Task Order Number	Mileage Band Low	Mileage Band High	Fixed Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.1.3.2.3 OCONUS OWS Transport Prices Table

CLIN	Case Number*	Task Order Number	Originating Country/ Jurisdiction ID**	Terminating Country/ Jurisdiction ID**	Mileage Band Low	Mileage Band High	Fixed Price	Variable Price Per Mile	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.1.3.2.4 Non-Domestic OWS Transport Prices Table (Optional)

CLIN	Case Number*	Task Order Number	Originating Country/ Jurisdiction ID**	Terminating Country/ Jurisdiction ID**	Mileage Band Low	Mileage Band High	Fixed Price	Variable Price Per Mile	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.1.3.2.5 OWS WDM Transport Pricing Instructions Table

MRC CLIN	Description	Charging Unit	Notes
OW00101	1 Gbps – Metro	Wavelength	
OW00102	OC48 – 2.5 Gbps – Metro	Wavelength	
OW00103	OC48c – 2.5 Gbps – Metro	Wavelength	
OW00104	OC192 – 10 Gbps – Metro	Wavelength	
OW00105	40 Gbps – Metro	Wavelength	ICB - Optional
OW00106	100 Gbps – Metro	Wavelength	ICB - Optional
OW00107	1 Gbps – Domestic Long Haul	Wavelength	
OW00108	OC48 – 2.5 Gbps – Domestic Long Haul	Wavelength	
OW00109	OC48c – 2.5 Gbps – Domestic Long Haul	Wavelength	
OW00110	OC192 – 10 Gbps – Domestic Long Haul	Wavelength	
OW00111	40 Gbps – Domestic Long Haul	Wavelength	ICB - Optional
OW00112	100 Gbps – Domestic Long Haul	Wavelength	ICB - Optional
OW00113	1 Gbps – Non-Domestic Long Haul	Wavelength	ICB - Optional
OW00114	OC48 – 2.5 Gbps – Non-Domestic Long Haul	Wavelength	ICB - Optional

MRC CLIN	Description	Charging Unit	Notes
OW00115	OC48c – 2.5 Gbps – Non-Domestic Long Haul	Wavelength	ICB - Optional
OW00116	OC192 – 10 Gbps – Non-Domestic Long Haul	Wavelength	ICB - Optional
OW00117	40 Gbps – Non-Domestic Long Haul	Wavelength	ICB - Optional
OW00118	100 Gbps – Non-Domestic Long Haul	Wavelength	ICB - Optional

B.2.1.3.3 OWS Features

Table B.2.1.3.3.1 provides the format for pricing information for OWS features for WDM. Table B.2.1.3.3.2 provides applicable charging mechanisms and charging units for OWS features.

B.2.1.3.3.1 OWS Feature Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.1.3.3.2 OWS WDM Feature Pricing Instructions Table

MRC CLIN	Description	Charging Unit	Notes
OW00301	Customer Network Management (CNM) – Level 1	Site	Optional. Network site identified by NSC
OW00302	Customer Network Management (CNM) – Level 2	Site	Optional. Network site identified by NSC
OW00303	Equipment Protection 1:1	Wavelength	ICB
OW00304	Equipment Protection 1+1	Wavelength	ICB
OW00305	Equipment Protection – Network Side	Wavelength	ICB
OW00306	Geographical Diversity – Wavelengths	Wavelength	ICB
OW00307	Protected CONUS Wavelength	Wavelength	Optional - ICB
OW00308	Protected OCONUS Wavelength	Wavelength	Optional - ICB
OW00309	Protected Non-Domestic Wavelength	Wavelength	Optional - ICB

MRC CLIN	Description	Charging Unit	Notes
OW00310	Protected Metro Wavelength	Wavelength	ICB

B.2.1.3.4 OWS Task Order Unique CLINs

Table B.2.1.3.4.1 provides the format for pricing TUCs supported by WDM. Table B.2.1.3.4.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.1.3.4.1 OWS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.1.3.4.2 OWS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
OW99990	OW99991	OW99992	OWS Task Order Unique	ICB	ICB

B.2.1.4 Private Line Service

The technical requirements for Private Line Service (PLS) are defined in Section C.2.1.4.

PLS provides facilities for duplex (bi-directional) service between two or more specified end points. Accordingly, PLS is priced without regard for direction of carried traffic. The two endpoints are designated by POPs (or other comparable locations) as defined in Section B.4.1. For convenience, the ends of a PLS circuit are referred to as “originating” and “terminating,” although these terms have no operational or pricing significance.

The price structure for PLS includes the following elements:

1. MRC per circuit for transport
2. Feature Charges

Domestic PLS transport prices shall be either a solely distance-based MRC or a combination of monthly recurring fixed price plus distance-based monthly recurring charges. Non-domestic PLS and ICB transport prices shall consist of a monthly recurring fixed price only (no per-mile charge). Where access is used to connect the

SDP to the contractor's designated connecting POP (or other comparable location), access prices shall be provided in accordance with Section B.2.9.

Prices for any associated SRE shall be provided in accordance with Section B.2.10.

In the case of multipoint PLS connections, the number and identities of the access and transport links shall be calculated using a least cost routing (e.g., minimal spanning tree) algorithm to determine the shortest overall distance to connect all POPs within the multipoint network. Distance between POPs shall be calculated using the distance formula listed in Section B.1.2.7. Each transport link in the minimal spanning tree shall be priced separately as described in Section B.2.1.4.1 and the prices summed to determine the total transport price.

For non-domestic PLS, fixed prices shall be provided for the full channel transport elements for countries where the contractor offers PLS on a full channel basis (see Table B.4.2.1 for Country/Jurisdiction IDs).

B.2.1.4.1 PLS Transport Prices

The PLS transport prices shall be determined as follows:

1. When both serving POPs are in the same country/jurisdiction (either CONUS or OCONUS), a price component from Table B.2.1.4.1.2 shall be used.
2. When one serving POP is within CONUS and the other is in OCONUS, two price components shall be used:
   a) A price (from Table B.2.1.4.1.2) for transport between the designated CONUS-serving POP and the PLS Gateway (from Table B.4.1.10 Domestic Private Line Service Gateways).
   b) A price (from Table B.2.1.4.1.3) for transport between designated PLS Gateway and the OCONUS service region.
3. When both serving POPs are in (different) OCONUS country/jurisdictions, a single price component from Table B.2.1.4.1.3 shall be used.
4. When one serving POP is in a non-domestic country/jurisdiction and the other is in a domestic service region (either CONUS or OCONUS), two price components shall be used:
   a) A price (from Table B.2.1.4.1.3) for transport between the non-domestic POP and the designated PLS Gateway (see Table B.4.1.11 Domestic Private Line Gateway to Non-Domestic Country/Jurisdiction Relationship).
   b) A price (from Table B.2.1.4.1.2) for domestic transport between the designated PLS gateway and the domestic serving POP.
5. When both serving POPs are in different non-domestic countries/jurisdictions, a single price component from Table B.2.1.4.1.3 shall be used.

6. When both serving POPs are in a single non-domestic country/jurisdiction, a single price component from Table B.2.1.4.1.4 shall be used.

Table B.2.1.4.1.1 lists the tables which define the appropriate formats for the PLS pricing scenarios described above.

B.2.1.4.1.1 PLS Summary of Pricing Tables Needed for Transport Pricing

	POP in CONUS	**POP in OCONUS**	**POP in Non-Domestic Country/Jurisdiction**
POP in CONUS	Table B.2.1.4.1.2~~B.2.1.4.1.2~~	Tables B.2.1.4.1.2~~B.2.1.4.1.2~~ and B.2.1.4.1.3~~B.2.1.4.1.3~~	Tables B.2.1.4.1.2~~B.2.1.4.1.2~~ and B.2.1.4.1.3~~B.2.1.4.1.3~~
POP in OCONUS	Tables B.2.1.4.1.2~~B.2.1.4.1.2~~ and B.2.1.4.1.3~~B.2.1.4.1.3~~	Same Country/Jurisdiction: Table B.2.1.4.1.2~~B.2.1.4.1.2~~ Different Country/Jurisdictions: Table B.2.1.4.1.3~~B.2.1.4.1.3~~	Tables B.2.1.4.1.2~~B.2.1.4.1.2~~ and B.2.1.4.1.3~~B.2.1.4.1.3~~
POP in Non-Domestic Country/Jurisdiction	Tables B.2.1.4.1.2~~B.2.1.4.1.2~~ and B.2.1.4.1.3~~B.2.1.4.1.3~~	Tables B.2.1.4.1.2~~B.2.1.4.1.2~~ and B.2.1.4.1.3~~B.2.1.4.1.3~~	Same Country/Jurisdiction: Table B.2.1.4.1.4~~B.2.1.4.1.4~~ Different Country/Jurisdictions: Table B.2.1.4.1.3~~B.2.1.4.1.3~~

Table B.2.1.4.1.2 provides the formats for pricing information for PLS domestic (same Country/Jurisdiction ID) transport service. The price may be either based solely on distance-based MRC or on a combination of a monthly recurring fixed price plus distance-based MRC. ICB transport prices shall consist of a monthly recurring fixed price only (no per-mile charge). Distance between the POPs shall be calculated using the distance formula in Section B.1.2.7.

When using distance-based pricing with minimum/maximum distance banding, monthly price per mile for the corresponding band shall be multiplied by the total transport distance in miles.

B.2.1.4.1.2 PLS Domestic Transport Prices Table

CLIN	Case Number*	Task Order Number	Mileage Band Low	Mileage Band High	Fixed Price	Variable Price per Mile**	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Price per mile not applicable to ICB CLINs

Table B.2.1.4.1.3 provides the pricing formats for PLS transport for OCONUS and non-domestic circuits between different countries/jurisdictions. Table B.2.1.4.1.4 provides the formats for PLS transport for non-domestic circuits within a single country/jurisdiction. POPs for intra-country/intra-jurisdiction non-domestic circuits shall be assigned to the closest POP to each location (based on distance) within that country/jurisdiction.

OCONUS POPs are listed in Table B.4.1.1; non-domestic POPs are listed in Table B.4.1.2. Domestic service gateways are listed in Table B.4.1.10. Country/Jurisdiction IDs are listed in Table B.4.2.1.

B.2.1.4.1.3 PLS OCONUS and Non-Domestic Transport Prices Table (Different Country Jurisdictions)

CLIN	Case Number*	Task Order Number	Country/ Jurisdiction ID (Originating)**	Country/ Jurisdiction ID (Terminating)**	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.1.4.1.4 PLS Non-Domestic Transport Prices Table (Same Country/Jurisdiction IDs)

CLIN	Case Number*	Task Order Number	Country/ Jurisdiction ID**	POP ID (Originating)	POP ID (Terminating)	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

Table B.2.1.4.1.5 provides applicable charging mechanisms and charging units for full channels.

B.2.1.4.1.5 PLS Full Channel Pricing Instructions Table

MRC CLIN	Description	Charging Unit	Notes
PL00101	Basic Subscriber Line (4 KHz)	Circuit	Optional
PL00102	DS0	Circuit	
PL00103	T1	Circuit	
PL00104	E1	Circuit	
PL00112	FT3 T1 x 2	Circuit	
PL00105	T3	Circuit	
PL00106	E3	Circuit	
PL00107	OC-3c	Circuit	
PL00108	OC-12c	Circuit	
PL00109	OC-48c	Circuit	ICB
PL00110	OC-192c	Circuit	ICB
PL00111	OC-768c	Circuit	ICB; optional

B.2.1.4.2 PLS Feature Prices

Table B.2.1.4.2.1 provides the formats for pricing information for PLS features. Table B.2.1.4.2.2 provides applicable charging mechanisms and charging units.

For PLS transport avoidance features, additional mileage shall be calculated as the difference between the avoidance route miles and the distance calculated using the V&H coordinate formula in Section B.1.2.7.

B.2.1.4.2.1 PLS Feature Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.1.4.2.2 PLS Feature Pricing Instructions Table

MRC CLIN	Description	Charging Unit	Notes
PL00201	Special Routing - Transport Diversity	Circuit	MRC is in addition to the transport circuit price that will apply to each transport circuit in each relationship pair.

MRC CLIN	Description	Charging Unit	Notes
PL00202	Special Routing - Transport Avoidance	Mile	MRC is in addition to the transport circuit price that will apply without avoidance routing. It applies only to the excess mileage incurred by the avoidance-routed circuit(s).
PL00203	Multipoint Connections - Branch-Off	Multipoint drop	MRC applies only to multipoint drops provided within the transport component
PL00204	Multipoint Connections - Drop and Insert	Multipoint drop	MRC applies only to multipoint drops provided within the transport component
PL00205	Channelized Circuits	Circuit	NSP. Contractor shall use this CLIN to indicate that a channelized or non-concatenated circuit is being ordered (instead of un-channelized or concatenated) at no additional cost.

B.2.1.4.3 PLS Task Order Unique CLINs

Table B.2.1.4.3.1 provides the format for pricing TUCs supported by PLS. Table B.2.1.4.3.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.1.4.3.1 PLS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.1.4.3.2 PLS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
PL99990	PL99991	PL99992	PLS Task Order Unique	ICB	ICB

B.2.1.5 Synchronous Optical Network Service

The technical requirements for Synchronous Optical Network Service (SONETS) are defined in Section C.2.1.5.

B.2.1.5.1 Access

The contractor shall price access to SONETS separately, when required. The contractor shall list all access charges for SONETS in B.2.9. Prices for any associated SRE shall be provided in accordance with Section B.2.10.

B.2.1.5.2 SONETS Task Order Unique CLINs

Table B.2.1.5.2.1 provides the format for pricing TUCs supported by SONETS. Table B.2.1.5.2.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.1.5.2.1 SONETS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.1.5.2.2 SONETS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
SO99990	SO99991	SO99992	SONETS Task Order Unique	ICB	ICB

B.2.1.6 Dark Fiber Service

The technical requirements for Dark Fiber Service (DFS) are defined in Section C.2.1.6.

B.2.1.6.1 DFS Price Structure

The price structure for DFS includes the following elements:

1. MRC for the Indefeasible Rights of Use (IRU) for on-net connections or along routes where fiber is installed, per fiber pair for transport
2. Feature Charges

Where access is used to connect the SDP to the contractor's designated connecting POP, access prices shall be provided in accordance with Section B.2.9.

Prices for any associated SRE shall be provided in accordance with Section B.2.10.

B.2.1.6.2 DFS Transport

The MRC includes the IRU for the use of the fiber, not the actual fiber itself. The MRC may vary depending on the number of pairs of strands in the fiber cable. The MRC is comprised entirely of a fixed component. The management, ongoing monitoring

support, maintenance, and repair of DFS in case of breaks shall be included in the MRC. Table B.2.1.6.2.1 provides the formats for pricing information for DFS. Table B.2.1.6.2.2 provides the applicable charging mechanisms and charging units for DFS.

B.2.1.6.2.1 DFS Transport Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

*Applies only to ICB CLINs

B.2.1.6.2.2 DFS Pricing Instructions Table

MRC CLIN	Description	Charging Unit	Notes
DK00101	DFS – Fiber Pair – 1 Fiber Pair	Fiber Pair	ICB
DK00102	DFS – Fiber Pair – More than 1 Fiber Pair	Fiber Pair	ICB
DK00103	DFS – Fiber Pair – Non-domestic	Fiber Pair	ICB Optional

B.2.1.6.3 DFS Feature Prices

Table B.2.1.6.3.1 provides the formats for pricing information for DFS features. Table B.2.1.6.3.2 provides applicable charging mechanisms and charging units for DFS features. Cost for all other features will be part of the ICB Dark Fiber CLIN pricing (e.g., Duct, Multiple Duct, etc.).

B.2.1.6.3.1 DFS Feature Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.1.6.3.2 DFS Feature Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
DK09001		Colocation Service – Add/drop traffic (gateways) and to regenerate and amplify traffic	Gateway	ICB
	DK09002	Colocation Service – Add/drop traffic (gateways) and to regenerate and amplify traffic	Gateway	ICB

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
DK09003		Off-Net laterals	Proposal	ICB (one-time payment)
	DK09004	Off-Net laterals	Proposal	ICB (monthly installments)
DK09005		Splicing	Dispatch	ICB

B.2.1.6.4 DFS Task Order Unique CLINs

Table B.2.1.6.4.1 provides the format for pricing TUCs supported by DFS. Table B.2.1.6.4.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.1.6.4.1 DFS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.1.6.4.2 DFS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
DK99990	DK99991	DK99992	DFS Task Order Unique	ICB	ICB

B.2.1.7 Internet Protocol Service (IPS)

The technical requirements for Internet Protocol Service (IPS) are defined in Section C.2.1.7.

All configurations of Quality of Service (QoS) are defined in Section C.2.1.7.2. QoS shall be included in the port price (i.e., NSP). Since QoS is also ICB, a case number shall be assigned for each port purchase and a description shall be provided of how the port will be configured.

B.2.1.7.1 IPS Price Structure

The price structure for domestic and non-domestic IPS includes the following elements:

1. MRC per Port
2. Feature Charges

Prices for any associated SRE shall be provided in accordance with Section B.2.10.

B.2.1.7.2 IPS Access

The contractor shall allow a government agency to connect to the contractor's IPS transport network using either of the following access methods:

1. Non-embedded access
2. Embedded access

B.2.1.7.2.1 Non-embedded Access

Where non-embedded access is used to connect the SDP to the contractor's designated connecting POP, non-embedded access prices shall be provided in accordance with Section B.2.9.

B.2.1.7.2.2 Embedded Access

When services such as DSL or Cable High-Speed are offered as embedded access by the contractor, the service price shall be included in the contractor's port price. See Section J.1 for the geographical scope of these service offerings.

B.2.1.7.3 IPS Port Prices

Table B.2.1.7.3.1 provides the format for pricing IPS. Table B.2.1.7.3.2 provides the pricing mechanisms and charging units.

Domestic access will connect to the contractor's IPS network through a domestic access port. The contractor shall price domestic access ports based on a monthly recurring charge.

Non-domestic access will connect to the contractor's IPS network through a non-domestic access port. The contractor shall price non-domestic access ports based on a monthly recurring charge.

The Country/Jurisdiction IDs are provided in Table B.4.2.1.

B.2.1.7.3.1 IPS Port Prices Table

CLIN	Case Number*	Task Order Number	Country/ Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Case number applies to ICB CLINs only

** For Country/Jurisdiction ID codes, see Section B.6.6

B.2.1.7.3.2 IPS Port Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
IP10001	MRC	IPS – T1 – 1.5 Mbps	Port	
IP10002	MRC	IPS – 2 x T1 – 3 Mbps	Port	
IP10003	MRC	IPS – 4 x T1 – 6 Mbps	Port	
IP10004	MRC	IPS – 6 x T1 – 9 Mbps	Port	
IP10010	MRC	IPS – FT3 – 3 Mbps	Port	
IP10012	MRC	IPS – FT3 – 6 Mbps	Port	
IP10013	MRC	IPS – FT3 – 9 Mbps	Port	
IP10014	MRC	IPS – FT3 – 15 Mbps	Port	
IP10015	MRC	IPS – FT3 – 24 Mbps	Port	
IP10016	MRC	IPS – FT3 – 30 Mbps	Port	
IP10019	MRC	IPS – T3 – 45 Mbps	Port	
IP10020	MRC	IPS – OC3c (155 Mbps)	Port	
IP10021	MRC	IPS – OC12c (622 Mbps)	Port	
IP10022	MRC	IPS – OC48c (2.5 Gbps)	Port	
IP10023	MRC	IPS – OC192c (10 Gbps)	Port	
IP10031	MRC	IPS – Ethernet – 1 Mbps	Port	
IP10032	MRC	IPS – Ethernet – 3 Mbps	Port	
IP10033	MRC	IPS – Ethernet – 6 Mbps	Port	
IP10036	MRC	IPS – Ethernet – 10 Mbps	Port	
IP10040	MRC	IPS – Ethernet – 20 Mbps	Port	
IP10041	MRC	IPS – Ethernet – 30 Mbps	Port	
IP10042	MRC	IPS – Ethernet – 40 Mbps	Port	
IP10043	MRC	IPS – Ethernet – 50 Mbps	Port	
IP10049	MRC	IPS – Ethernet – 100 Mbps	Port	
IP10050	MRC	IPS – Ethernet – 200 Mbps	Port	

CLIN	Frequency	Description	Charging Unit	Notes
IP10051	MRC	IPS – Ethernet – 300 Mbps	Port	
IP10052	MRC	IPS – Ethernet – 400 Mbps	Port	
IP10053	MRC	IPS – Ethernet – 500 Mbps	Port	
IP10059	MRC	IPS – Ethernet – 1 Gbps	Port	
IP10061	MRC	IPS – Ethernet – 2 Gbps	Port	
IP10062	MRC	IPS – Ethernet – 3 Gbps	Port	
IP10069	MRC	IPS – Ethernet – 10 Gbps	Port	
IP10070	MRC	IPS – E1 NONDOM	Port	
IP10071	MRC	IPS – E1 CONUS/OCONUS	Port	Optional
IP10080	MRC	IPS – E3 NONDOM	Port	
IP10081	MRC	IPS – E3 CONUS/OCONUS	Port	Optional
IP20001	MRC	IPS – SDSL – up to 1.5 Mbps	Port	Embedded Access. Optional
IP21001	MRC	IPS – ADSL – up to 1.5 Mbps download	Port	Embedded Access. Optional
IP21002	MRC	IPS – ADSL – up to 5 Mbps download	Port	Embedded Access. Optional
IP21003	MRC	IPS – ADSL – up to 8 Mbps download	Port	Embedded Access. Optional
IP30001	MRC	IPS – T3 burstable – 5 Mbps committed	Port	
IP30002	MRC	IPS – T3 burstable – 10 Mbps committed	Port	
IP30003	MRC	IPS – T3 burstable – 15 Mbps committed	Port	
IP30004	MRC	IPS – T3 burstable – 20 Mbps committed	Port	
IP30005	MRC	IPS – T3 burstable – 30 Mbps committed	Port	
IP30008	Usage	T3 burstable overage	Mbps	
IP30010	MRC	IPS – Ethernet – 20 Mbps committed, burstable to 100 Mbps	Port	
IP30011	MRC	IPS – Ethernet – 30 Mbps committed, burstable to 100 Mbps	Port	
IP30012	MRC	IPS – Ethernet – 40 Mbps committed, burstable to 100 Mbps	Port	

CLIN	Frequency	Description	Charging Unit	Notes
IP30013	MRC	IPS – Ethernet – 50 Mbps committed, burstable to 100 Mbps	Port	
IP30021	MRC	IPS – Ethernet – 200 Mbps committed, burstable to 1 Gbps	Port	
IP30022	MRC	IPS – Ethernet – 300 Mbps committed, burstable to 1 Gbps	Port	
IP30023	MRC	IPS – Ethernet – 400 Mbps committed, burstable to 1 Gbps	Port	
IP30024	MRC	IPS – Ethernet – 500 Mbps committed, burstable to 1 Gbps	Port	
IP30025	MRC	IPS – Ethernet – 600 Mbps committed, burstable to 1 Gbps	Port	
IP40020	Usage	IPS – Ethernet burstable overage for 20 Mbps committed port burstable to 100 Mbps	Mbps	
IP40030	Usage	IPS – Ethernet burstable overage for 30 Mbps committed port burstable to 100 Mbps	Mbps	
IP40040	Usage	IPS – Ethernet burstable overage for 40 Mbps committed port burstable to 100 Mbps	Mbps	
IP40050	Usage	IPS – Ethernet burstable overage for 50 Mbps committed port burstable to 100 Mbps	Mbps	
IP40200	Usage	IPS – Ethernet burstable overage for 200 Mbps committed port burstable to 1 Gbps	Mbps	
IP40300	Usage	IPS – Ethernet burstable overage for 300 Mbps committed port burstable to 1 Gbps	Mbps	
IP40400	Usage	IPS – Ethernet burstable overage for 400 Mbps committed port burstable to 1 Gbps	Mbps	
IP40500	Usage	IPS – Ethernet burstable overage for 500 Mbps committed port burstable to 1 Gbps	Mbps	
IP40600	Usage	IPS – Ethernet burstable overage for 600 Mbps committed port burstable to 1 Gbps	Mbps	
IP50001	MRC	IP Quality of Service (QoS)	Port	NSP, ICB

Satellite internet access services shall be provided in accordance with Section B.2.7.

Wireless (LTE) internet access services shall be provided in accordance with Section B.2.6.

Managed Trusted Internet Protocol Services (MTIPS) shall be provided in accordance with Section B.2.8.4.

Burstable bandwidth allows an agency to subscribe to a bandwidth commitment that is less than the full bandwidth of the selected IPS port, but may burst to the full bandwidth of the selected port. The bandwidth commitment equals the portion capacity of a circuit (as measured in bandwidth) that an agency may use in a monthly period without

incurring an overage charge. A T3 burstable or Ethernet burstable CLIN shall guarantee a committed bandwidth while ensuring the availability of the increased capacity.

Bandwidth used in excess of the committed burstable bandwidth shall be invoiced via an overage usage CLIN. For each T3 burstable or Ethernet burstable MRC CLIN, a corresponding burstable overage usage CLIN shall be auto-sold to simplify ordering. For example, Ethernet burstable overage CLIN IP40030 shall be auto-sold with Ethernet burstable transport CLIN IP30011, and T3 burstable overage CLIN IP30008 shall be auto-sold with T3 burstable CLIN IP30003.

With burstable bandwidth, agencies shall only be charged for the amount of bandwidth used on a sustained level (95th percentile). Bandwidth shall be measured (or sampled) from the switch or router every 5 minutes. At the end of the month, the top 5% of data shall be discarded. The next highest measurement shall determine the billable usage for the month. Overages shall be billed in one-megabit per second increments for usage above the selected bandwidth commitment.

B.2.1.7.4 IPS Feature Prices

Table B.2.1.7.4.1 provides the format for pricing the features supported by IPS.

B.2.1.7.4.1 IPS Feature Prices Table (Reserved for future use)

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.1.7.5 IPS Task Order Unique CLINs

Table B.2.1.7.5.1 provides the format for pricing the TUCs supported by IPS. Table B.2.1.7.5.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.1.7.5.1 IPS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.1.7.5.2 IPS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
IP99990	IP99991	IP99992	IPS Task Order Unique	ICB	ICB

B.2.2 Voice Service

The technical requirements for Voice Service are defined in Sections C.2.2.1 and C.2.2.2.

Voice Service can be provided using various technologies. The pricing tables have been organized as follows:

1. Internet Protocol Voice Service (IPVS)
2. Circuit Switched Voice Service (CSVS)

Contractors shall propose prices for at least one of the Voice Service technologies specified above. Contractors shall price all mandatory CLINs associated with each technology proposed.

Price tables, associated CLINs and pricing instructions for each Voice Service technology are specified in the subsequent sub-sections.

B.2.2.1 Internet Protocol Voice Service

Internet Protocol Voice Service (IPVS) shall be used in conjunction with VPN or another transport service specified in this document. Pricing for VPNS is not included with IPVS, and can be found in Section B.2.1.1.

IPVS provides voice communications service and telephony features. Within IPVS, the following service options are available:

1. IPVS (Includes unlimited on-net to on-net and unlimited CONUS on-net to CONUS off-net calling):
   a) Hosted.
   b) Premises-Based.
2. Managed LAN (Requires IPVS).
3. Session Initiation Protocol (SIP) Trunk Service.

Contractors shall propose pricing for IPVS, Managed LAN and SIP Trunk Service. All CLINs are mandatory unless otherwise specified.

B.2.2.1.1 IPVS Price Structure

The price structure for IPVS includes the following components:

1. Basic service per telephone number (Includes unlimited on-net to on-net and unlimited CONUS on-net to CONUS off-net calling)
2. Per six-second off-net usage
3. Features

B.2.2.1.2 IPVS Prices

The contractor shall provide pricing information for IPVS in the formats specified in Tables B.2.2.1.2.1 and B.2.2.1.2.2. Available service types are provided in Table B.2.2.1.2.3.

B.2.2.1.2.1 IPVS CONUS Prices Table

CLIN	Case Number*	Task Order Number	Band Low**	Band High**	Variable Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items
** Banded pricing per charging unit. Contractor may propose pricing for multiple bands using the same CLIN.

B.2.2.1.2.2 IPVS OCONUS or Non-Domestic Prices Table

CLIN	Case Number*	Task Order Number	Originating Country/ Jurisdiction ID**	Band Low***	Band High***	Variable Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items
** Country/Jurisdiction IDs are provided in Table B.4.2.1
*** Banded pricing per charging unit. Contractor may propose pricing for multiple bands using the same CLIN.

B.2.2.1.2.3 IPVS Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
VI21110	VI22110	IPVS - Hosted	Seat	Includes unlimited on-net to on-net and unlimited CONUS on-net to CONUS off-net calling. For service implementations located in an OCONUS country/jurisdiction, unlimited off-net calling within the same OCONUS country/jurisdiction shall also be included.

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
VI21210	VI22210	IPVS - Premises-Based	Seat	Includes unlimited on-net to on-net and unlimited CONUS on-net to CONUS off-net calling. For service implementations located in an OCONUS country/jurisdiction, unlimited off-net calling within the same OCONUS country/jurisdiction shall also be included.

B.2.2.1.3 IPVS Off-Net Usage Prices

Contractors shall use the formats specified in Table B.2.2.1.3.1 to provide off-net termination pricing to all OCONUS and non-domestic countries/jurisdictions specified in Table J.1.2.1.

Where the contractor provides voice service to a particular country/jurisdiction, the prices in Tables B.2.2.1.3.1, B.2.2.1.3.2 and B.2.2.1.3.3 cannot be higher than the prices resulting from applying the multiple usage increments applicable to that country/jurisdiction as provided in Table B.2.2.2.1.3~~B.2.2.2.1.3~~. The originating country/jurisdiction is included in Table B.4.2.1.

Formatte

The price table and instructions for non-domestic mobile terminations are provided in Section B.2.2.1.3.5.

Off-net termination usage based pricing shall apply to IPVS with or without Managed LAN.

B.2.2.1.3.1 IPVS CONUS to OCONUS and Non-Domestic Off-Net Termination Usage Prices Table

CLIN	Task Order Number	Terminating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.1.3.2 IPVS OCONUS or Non-Domestic to CONUS Off-Net Termination Usage Prices Table

CLIN	Task Order Number	Originating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.1.3.3 IPVS OCONUS or Non-Domestic to OCONUS or Non-Domestic Off-Net Termination Usage Prices Table

CLIN	Task Order Number	Originating Country/ Jurisdiction ID*	Terminating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.1.3.4 IPVS On-Net to Off-Net Termination Usage Pricing Instructions Table

Usage CLIN	Description	Charging Unit	Notes
VI23010	IPVS: On-net to off-net calling	6 seconds	See Table B.2.2.2.1.3~~B.2.2.2.1.3~~ Usage Increments for applicable increments of 6 second usage.

Formatte

B.2.2.1.3.5 IPVS Non-Domestic Mobile Termination Surcharge

Contractors shall provide mobile termination pricing to all non-domestic countries/jurisdictions listed in Table J.1.2.1 except for satellite locations, which are the NONDOM locations in Table B.4.2.1 with no AOW ID. Table B.2.2.1.3.5.1 provides the formats for pricing information for IPVS non-domestic mobile termination add-on prices. Table B.2.2.1.3.5.2 provides applicable charging mechanisms and charging units for IPVS non-domestic mobile termination add-on prices.

B.2.2.1.3.5.1 IPVS Non-Domestic Mobile Termination Surcharge Prices Table

CLIN	Task Order Number	Terminating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.1.3.5.2 IPVS Non-Domestic Mobile Termination Surcharge Pricing Instructions Table

Usage CLIN	Description	Charging Unit
VI24000	Non-Domestic Mobile Termination Surcharge	6 seconds

B.2.2.1.4 IPVS Feature Prices

IPVS shall include the following features in the basic service price in Section B.2.2.1.2:

- Automatic Number Identification (ANI)
- 3-way Conference Calling
- Do Not Disturb

- Call Forward – All
- Call Forward – Busy
- Call Forward - Don't Answer
- Call Hold
- Call Transfer
- Call Number Suppression
- IP Telephony Manager (Administrator)
- Call Park
- Call Pickup
- Class of Service Restriction
- Distinctive Ringing
- Call Waiting
- Specific Call Rejection
- IP Telephony Manager (Subscriber)
- Hotline
- Hunt Groups
- Multi-Line Appearance
- Directory Assistance
- Speed Dial
- Last Number Dialed

The contractor shall provide pricing information for IPVS features in the formats specified in Tables B.2.2.1.4.1 and B.2.2.1.4.2. Pricing instructions are provided in Table B.2.2.1.4.3. The contractor shall provide pricing information for IPVS banded features in the formats specified in Tables B.2.2.1.4.4 and B.2.2.1.4.5. Pricing instructions are provided in Table B.2.2.1.4.6.

B.2.2.1.4.1 IPVS CONUS Feature Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items

B.2.2.1.4.2 IPVS OCONUS and Non-Domestic Feature Prices Table

CLIN	Case Number*	Task Order Number	Originating Country/ Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items
** Country/Jurisdiction IDs are provided in Table B.4.2.1

Contractors shall propose pricing for all features unless specified otherwise. Features apply to IPVS.

B.2.2.1.4.3 IPVS Feature Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit
VI21410	VI22410	IPVS: Voice Mail Box	Seat
VI21415	VI22415	IPVS: Auto Attendant	Instance*

* An Instance of IPVS: Auto Attendant is an auto attendant implementation containing the capabilities specified in Section C.2.2.1.2

B.2.2.1.4.4 IPVS CONUS Banded Feature Prices Table

CLIN	Case Number*	Task Order Number	Band Low**	Band High**	Variable Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items
** Banded pricing per charging unit. Contractor may propose pricing for multiple bands using the same CLIN.

B.2.2.1.4.5 IPVS OCONUS and Non-Domestic Banded Feature Prices Table

CLIN	Case Number*	Task Order Number	Originating Country/ Jurisdiction ID**	Band Low***	Band High***	Variable Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items
** Country/Jurisdiction IDs are provided in Table B.4.2.1
*** Banded pricing per charging unit. Contractor may propose pricing for multiple bands using the same CLIN.

Contractors shall propose pricing for all features unless specified otherwise. Features apply to IPVS.

B.2.2.1.4.6 IPVS Banded Feature Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
VI21420	VI22420	IPVS: PSAP Connection	Seat	Establish and maintain the connection to the PSAP and build out of the Private Switch/Automatic Location Identification (PS/ALI) database. Includes Remote Access Banded pricing per charging unit. Contractor may propose pricing for multiple bands using the same CLIN.

B.2.2.1.5 Managed LAN

IPVS is a pre-requisite for Managed LAN. IPVS shall be used in conjunction with a separately priced, VPN or another transport services specified in this document and shall be provided as described in Section C.2.1.4.1.

The contractor shall be responsible for providing and managing all Managed LAN networking hardware components (e.g. layer 2 switching devices, routers, call servers, etc.) to extend the IPVS from the site demarcation point to the terminating subscriber device. Managed LAN per seat pricing shall include all equipment necessary to provide the Managed LAN solution.

The contactor shall provide pricing information for Managed LAN basic service in the formats specified in Tables B.2.2.1.5.1~~B.2.2.1.5.1~~ and B.2.2.1.5.2~~B.2.2.1.5.2~~.

Formatte
Formatte

B.2.2.1.5.1 Managed LAN CONUS Prices Table

CLIN	Case Number*	Task Order Number	Band Low**	Band High**	Variable Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items
** Banded pricing per charging unit. Contractor may propose pricing for multiple bands using the same CLIN.

B.2.2.1.5.2 Managed LAN OCONUS or Non-Domestic Prices Table

CLIN	Case Number*	Task Order Number	Originating Country/ Jurisdiction ID**	Band Low***	Band High***	Variable Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items
** Country/Jurisdiction IDs are provided in Table B.4.2.1
*** Banded pricing per charging unit. Contractor may propose pricing for multiple bands using the same CLIN.

B.2.2.1.5.3 Managed LAN Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit
VI21310	VI22310	Managed LAN Without Call Server & Maintenance - Hosted	Seat

NRC CLIN	MRC CLIN	Description	Charging Unit
VI21320	VI22320	Managed LAN Service With Call Server & Maintenance - Premises-Based	Seat

B.2.2.1.6 Session Initiation Protocol Trunk Service

B.2.2.1.6.1 Session Initiation Protocol Trunk Price Structure

SIP Trunk service shall be priced using the following components. Charges for access arrangements shall not be included in SIP Trunk Service pricing, but shall be provided as described in Section C.2.2.1.6.

1. Basic Service (Includes unlimited on-net to on-net and unlimited CONUS on-net to CONUS off-net calling)
2. Off-net usage billed in six-second increments
3. Features

The network and the management of the network will be provided by the underlying network service. The equipment necessary to enable SIP Trunk service, such as gateways, routers, etc., shall be listed and priced as described in Section B.2.10.

Contractors shall propose pricing for SIP Trunk mandatory CLINs unless otherwise specified.

B.2.2.1.6.2 SIP Trunk CONUS Prices Table

CLIN	Case Number*	Task Order Number	Band Low**	Band High**	Variable Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items
** Banded pricing per charging unit. Contractor may propose pricing for multiple bands using the same CLIN.

B.2.2.1.6.3 SIP Trunk OCONUS or Non-Domestic Prices Table

CLIN	Case Number*	Task Order Number	Originating Country/ Jurisdiction ID**	Band Low***	Band High***	Variable Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items
** Country/Jurisdiction IDs are provided in Table B.4.2.1
*** Banded pricing per charging unit. Contractor may propose pricing for multiple bands using the same CLIN.

B.2.2.1.6.4 SIP Trunk Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
VI31110	VI32110	SIP Trunk: Basic Service	Concurrent call path	Includes unlimited on-net to on-net and unlimited CONUS on-net to CONUS off-net calling. For service implementations located in an OCONUS country/jurisdiction, unlimited off-net calling within the same OCONUS country/jurisdiction shall also be included.

B.2.2.1.7 SIP Trunk Off-Net Usage Pricing

Unlimited on-net to on-net and unlimited CONUS on-net to CONUS off-net calling shall be included with SIP Trunk Basic Service.

Contractors shall use the formats specified in Table B.2.2.1.7.1 to provide off-net termination pricing to all OCONUS and non-domestic countries/jurisdictions specified in Table J.1.2.1.

Where the contractor provides voice service to a particular country/jurisdiction, the prices in Tables B.2.2.1.7.1~~B.2.2.1.7.1~~, B.2.2.1.7.2 and B.2.2.1.7.3 cannot be higher than the prices resulting from applying the multiple usage increments applicable to that country/jurisdiction as provided in Table B.2.2.2.1.3~~B.2.2.2.1.3~~. The originating country/jurisdiction is included in Table B.4.2.1.

Formatte

Formatte

The price table and instructions for non-domestic mobile terminations are provided in Section B.2.2.1.3.5.

B.2.2.1.7.1 SIP Trunk CONUS On-Net to Off-Net OCONUS or Non-Domestic Usage-Based Prices Table

CLIN	Task Order Number	Terminating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.1.7.2 SIP Trunk OCONUS or Non-Domestic On-Net to OCONUS or Non-Domestic Off-Net Usage-Based Prices Table

CLIN	Task Order Number	Originating Country/ Jurisdiction ID*	Terminating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.1.7.3 SIP Trunk OCONUS or Non-Domestic On-Net to CONUS Off-Net Usage-Based Prices Table

CLIN	Task Order Number	Originating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.1.7.4 SIP Trunk On-Net to Off-Net Usage-Based Pricing Instructions Table

Usage CLIN	Description	Charging Unit	Notes
VI33010	SIP Trunk: On-Net to Off-Net Calling	6 seconds	See Table B.2.2.2.1.3~~B.2.2.2.1.3~~ Usage Increments for applicable increments of 6 second usage.

Formatte

B.2.2.1.8 SIP Trunk Feature Prices

The contractor shall provide pricing information for SIP Trunk features in the formats specified in Tables B.2.2.1.8.1 and Tables B.2.2.1.8.2. Pricing instructions are provided in Table B.2.2.1.8.3.

B.2.2.1.8.1 SIP Trunk CONUS Standard Feature Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items

B.2.2.1.8.2 SIP Trunk OCONUS or Non-Domestic Feature Prices Table

CLIN	Case Number*	Task Order Number	Originating Country/ Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.1.8.3 SIP Trunk Standard Feature Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
VI31410	VI32410		SIP Trunk: Automatic call routing	Concurrent call path	
VI31415	VI32415		SIP Trunk: Bandwidth QOS Management	Trunk	
VI31420	VI32420		SIP Trunk: Trunk Bursting*	Trunk	
VI31425	VI32425		SIP Trunk: ~~Telephone~~Single DID Number Assignment and Maintenance	Number	
VI31430	VI32430		SIP Trunk: Block of 10 DID Numbers Assignment and Maintenance	Block	
VI31435	VI32435		SIP Trunk: Block of 100 DID Numbers Assignment and Maintenance	Block	
VI31440	VI32440		SIP Trunk: Block of 1000 DID Numbers Assignment and Maintenance	Block	
VI31445			SIP Trunk: DID Number Capture	Number	NSP. CLIN shall be ordered as many times as necessary to record all detailed information required in Section J.2 for each DID Number ordered via VI31430, VI31435, or VI31440.
		VI33445	SIP Trunk: Burstable Call Path**	Concurrent call path	

* SIP Trunk: Trunk Bursting feature provides the capability to burst additional call path(s) within a trunk.

**SIP Trunk: Burstable Call Path feature is the utilization of an additional call path within a trunk. For each burstable call path utilized, one usage charge shall be billed per month regardless of the number of bursting instances occurred within the same month. Requires SIP Trunk: Trunk Bursting CLINs.

B.2.2.1.9 IPVS Task Order Unique CLINs

Table B.2.2.1.9.1 provides the format for pricing TUCs for IPVS. Table B.2.2.1.9.2 provides IPVS TUC pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.2.1.9.1 IPVS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.2.1.9.2 IPVS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
VI99990	VI99991	VI99992	IPVS Task Order Unique	ICB	ICB

B.2.2.2 Circuit Switched Voice Service

Circuit Switched Voice Service (CSVS) supports both traditional local and long distance service. Prices may vary based on originating technology.

The mandatory price structure for CSVS includes the following elements:

1. Usage including switched originating access and/or terminating access costs, as applicable, per six-second increment. Unlimited CONUS to CONUS or within the same OCONUS country/jurisdiction calling service packages are also available.
2. Features.

Usage charges for calls to non-domestic and OCONUS countries/jurisdictions shall be charged at the usage rates provided in Section B.2.2.2.1.1. Contractors shall use Table B.2.2.2.1.6 to provide off-net termination pricing to all OCONUS and non-domestic countries/jurisdictions specified in Table J.1.2.1. Additionally, contractors shall provide pricing for all the OCONUS and non-domestic countries/jurisdictions specified in Table B.4.2.1 where the service will be offered.

All CSVS usage-based prices shall be billed in six-second increments unless otherwise specified. A minimum number of billing increments per call shall be set at the levels defined in B.2.2.2.1.3.

Charges for access arrangements (e.g. Basic Subscriber Line, ISDN PRI, and ISDN BRI) shall not be included in CSVS pricing, but shall be provided as described in Section B.2.9.

Contractors shall provide pricing for all Voice Service Basic CLINs unless specified otherwise.

B.2.2.2.1 Circuit Switched Voice Service Usage

Contractors shall propose CSVS pricing to support six-second increment, usage-based, and Unlimited CONUS to CONUS or within the same OCONUS country/jurisdiction scenarios. Section B.2.2.2.1.1 provides pricing tables and instructions for six-second increment usage-based pricing including CONUS to CONUS.

Unlimited CONUS to CONUS or within the same OCONUS country/jurisdiction Plans require Basic Subscriber Line, ISDN PRI or Voice Service ISDN BRI access. Table B.2.2.2.1.4 provides pricing tables and instructions for Unlimited CONUS to CONUS or within the same OCONUS country/jurisdiction Plans. Section B.2.9 provides Access pricing.

B.2.2.2.1.1 CSVS Usage-Based Prices

Usage-based pricing shall be on a country/jurisdiction-to-country/jurisdiction basis between the countries involved in the call. The pricing tables applicable to all categories of CONUS, OCONUS and non-domestic transport are listed in Table B.2.2.2.1.4. The following types of calls are differentiated:

1. CONUS to CONUS.
2. CONUS to OCONUS or non-domestic.
3. OCONUS or non-domestic to CONUS.
4. OCONUS or non-domestic to OCONUS or non-domestic.
5. Non-domestic mobile termination.

Contractors shall use the following pricing instructions for CONUS, OCONUS and non-domestic CSVS Usage-Based pricing tables.

B.2.2.2.1.2 CSVS Usage-Based Pricing Instructions Table

Usage CLIN	Description	Charging Unit	Notes
VS13010	Switched access origination	6 seconds	
VS13020	Dedicated access origination	6 seconds	Examples of Dedicated Access include, but are not limited to, Basic Subscriber Line, ISDN PRI, and ISDN BRI.

Minimum Billing Increments for CSVS Usage-Based Billing shall be priced in six-second increments. The number of minimum increments per call varies based on call type.

B.2.2.2.1.3 Usage Increments

From	To	Minimum Increments Per Call
Domestic (CONUS/OCONUS)	Domestic (CONUS/OCONUS)	One
Domestic (CONUS/OCONUS)	Non-domestic	Three
Non-domestic	Domestic (CONUS/OCONUS)	Five
Non-domestic	Non-domestic	Five

CONUS, OCONUS and Non-Domestic Usage-Based Pricing Tables can be found using the Cross-Reference Table B.2.2.2.1.4.

B.2.2.2.1.4 Usage Pricing Cross Reference

Transport Category	From Location	To Location	Table
Outbound	CONUS	CONUS	B.2.2.2.1.5
Outbound	CONUS	OCONUS or Non-domestic	B.2.2.2.1.6
Inbound	OCONUS or Non-domestic	CONUS	B.2.2.2.1.7
Non-domestic to Non-domestic	OCONUS or Non-domestic	OCONUS or Non-domestic	B.2.2.2.1.8

For non-domestic mobile termination calls, a per six-second increment additional add-on charge shall apply to certain non-domestic telephone calls that terminate to a mobile phone or other wireless devices. These add-ons vary by country.

B.2.2.2.1.5 CSVS CONUS to CONUS Usage-Based Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.2.2.1.6 CSVS CONUS to OCONUS or Non-Domestic Usage-Based Prices Table

CLIN	Task Order Number	Terminating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.2.1.7 CSVS OCONUS or Non-Domestic to CONUS Usage-Based Prices Table

CLIN	Task Order Number	Originating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.2.1.8 CSVS OCONUS or Non-Domestic to OCONUS or Non-Domestic Usage-Based Prices Table

CLIN	Task Order Number	Originating Country/ Jurisdiction ID*	Terminating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

For each originating OCONUS country/jurisdiction priced in Table B.2.2.2.1.8, the contractor shall price terminations to all OCONUS and non-domestic countries/jurisdictions specified in Table J.1.2.1.

B.2.2.2.1.9 CSVS Non-Domestic Mobile Termination Surcharge

Contractors shall provide mobile termination pricing to all non-domestic countries/jurisdictions listed in Table J.1.2.1 except for satellite locations, which are the NONDOM locations in Table B.4.2.1 with no AOW ID.Table B.2.2.2.1.9.1 provides the formats for pricing information for CSVS non-domestic mobile termination add-on

prices. Table B.2.2.2.1.9.2 provides applicable charging mechanisms and charging units for CSVS non-domestic mobile termination add-on prices.

B.2.2.2.1.9.1 CSVS Non-Domestic Mobile Termination Surcharge Prices Table

CLIN	Task Order Number	Terminating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.2.1.9.2 CSVS Non-Domestic Mobile Termination Surcharge Pricing Instructions Table

Usage CLIN	Description	Charging Unit
VS13030	Non-Domestic Mobile Termination Surcharge	6 seconds

B.2.2.2.2 CSVS Unlimited CONUS or OCONUS Calling Plan Prices

Unlimited Calling Plans shall be available when ordered with EIS Basic Subscriber Line, ISDN PRI or ISDN BRI access. Tables B.2.2.2.2.1 and B.2.2.2.2.2 provide pricing tables and instructions for Unlimited Calling Plans. Unlimited Calling Plans shall include:

1. Unlimited on-net to on-net and unlimited CONUS on-net to CONUS off-net calling.
2. Unlimited off-net calling within the same OCONUS country/jurisdiction, for service implementations located in an OCONUS country/jurisdiction.

Access prices shall be provided in accordance with Section B.2.9.

B.2.2.2.2.1 CSVS Unlimited CONUS or OCONUS Calling Plan Prices Table

CLIN	Task Order Number	Country/Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.2.2.2 CSVS Unlimited CONUS or OCONUS Calling Plan Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
VS11110	VS12110	Basic Subscriber Line: Unlimited Calling	Line	Includes the following features: 1. Call Transfer-All Calls 2. Call Hold 3. Three-Way Calling

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
				4. Intercom (Station-to-Station Dialing) 5. Direct Inward and Outward Dialing 6. Call Forwarding 7. Access Codes 8. Caller ID 9. Call Waiting
VS11210	VS12210	ISDN PRI: Unlimited Calling	Trunk	Includes the following features: 1. Block Exchanges 2. Data Call Setup 3. Data Line Privacy 4. Distinctive Ringing 5. Flexible Disconnect, Both/Either Party 6. Foreign Exchange Service 7. Six-Way Conference Call 8. Trunk Group Denial 9. Call Forwarding 10. Call Waiting
VS11310	VS12310	ISDN BRI: Unlimited Calling	Line	Includes the following features: 1. Call Transfer-All Calls 2. Call Hold 3. Three-Way Calling 4. Intercom (Station-to-Station Dialing) 5. Direct Inward and Outward Dialing 6. Access Codes 7. Call Forwarding 8. Call Waiting

B.2.2.2.3 CSVS Features

CSVS offers features for both Usage-Based and CONUS to CONUS or within the same OCONUS country/jurisdiction Unlimited Plan scenarios. Tables B.2.2.2.3.1 and B.2.2.2.3.2 shall be used to provide pricing for all features. The pricing instructions are categorized as follows:

1. General Features: Available to both six-second increment Usage-Based and Unlimited CONUS to CONUS or within the same OCONUS country/jurisdiction Plans.
2. Unlimited CONUS to CONUS or within the same OCONUS country/jurisdiction Plans:
   a) Basic Subscriber Line.
   b) ISDN PRI.
   c) ISDN BRI.

Where features are offered on other than CONUS to CONUS calls, the following pricing rules shall apply:

1. For features where normal call charges (basic service charges) also apply, the price applicable to the called country/jurisdiction (as determined by the called number) shall be used.
2. For features where normal call charges (basic service charges) do not apply, the price applicable to the calling country/jurisdiction shall be used (e.g., if locator service is offered in a specific country/jurisdiction, then the per-call price for that country/jurisdiction shall be used).

B.2.2.2.3.1 CSVS Features CONUS Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items

B.2.2.2.3.2 CSVS Features OCONUS and Non-Domestic Prices Table

CLIN	Task Order Number	Originating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

The following mandatory features, unless specified as optional, shall be priced for CSVS. This includes usage-based CONUS to CONUS per call and Unlimited Plan service categories.

B.2.2.2.3.3 CSVS General Features Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
	VS12410		Agency Recorded Announcements	Stored announcement	
VS14410			Authorization Codes/Post-paid Calling Card – Automated Verification	Automatic verification	Optional. Usage is billed via CSVS usage-based CLINs VS13010/VS13020.

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
					Normal call charges also apply to caller. Payphone surcharge applies to call made from payphones.
	VS12415		Caller ID	Number	If applicable
VS11420			General: Call Screening for Users – Class of Service (COS) and Restrictions	Restriction implemented or changed	
VS11425			Call Screening for Users – Code Block	Code block authorized or changed	Optional
VS11430	VS12430		Customized Network Announcement Intercept Scripts	Announcement	
		VS14420	Internal Agency Accounting Code	Call	Optional. Using Internal account identity code; normal call charges also apply to caller
		VS14425	Directory Assistance	Call	
VS11435	VS12435		Suppression of Calling Number Delivery	Implementation	NSP. Feature may be administered by number and/or by location

B.2.2.2.3.4 CSVS Unlimited CONUS or OCONUS Calling Plan Features Pricing Instructions

The following features are mandatory in addition to features specified in Table B.2.2.2.2.2, unless otherwise specified, for CSVS Unlimited CONUS or OCONUS Calling Plans. Pricing Instructions are provided per Unlimited CONUS or OCONUS Calling Plan.

B.2.2.2.3.4.1 CSVS Unlimited CONUS or OCONUS Plan-Basic Subscriber Line Features Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
VS11130	VS12130	Basic Subscriber Line: Multi Appearance Directory Number	Line	
VS11135	VS12135	Basic Subscriber Line: Voice Mail	Line	
VS11140	VS12140	Basic Subscriber Line: MLPP Feature	Line	Optional. Multi-Level Precedence and Preemption

B.2.2.2.3.4.2 CSVS Unlimited CONUS or OCONUS Plan-ISDN PRI Features Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
VS11230	VS12230	ISDN PRI: Backup of Shared-D Channel	Trunk	
VS11215	VS12215	ISDN PRI: Telephone Number Assignment and Maintenance	Number	
VS11220	VS12220	ISDN PRI: Voice Mail	Trunk	
VS11225	VS12225	ISDN PRI: MLPP Feature	Trunk	Optional. Multi-Level Precedence and Preemption
VS11235	VS12235	ISDN PRI: Block of 10 DID Numbers Assignment and Maintenance	Block	
VS11240	VS12240	ISDN PRI: Block of 100 DID Numbers Assignment and Maintenance	Block	
VS11245	VS12245	ISDN PRI: Block of 1000 DID Numbers Assignment and Maintenance	Block	

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
VS11250		ISDN PRI: DID Number Capture	Number	NSP. CLIN shall be ordered as many times as necessary to record all detailed information required in Section J.2 for each DID Number ordered via VS11235, VS11240, or VS11245.

B.2.2.2.3.4.3 CSVS Unlimited CONUS or OCONUS Plan- ISDN BRI Features Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
VS11315	VS12315	ISDN BRI: Multi Appearance Directory Number	Line	
VS11320	VS12320	ISDN BRI: Voice Mail	Line	
VS11325	VS12325	ISDN BRI: MLPP Feature	Line	Optional. Multi-Level Precedence and Preemption

B.2.2.2.4 CSVS Task Order Unique CLINs

Table B.2.2.2.4.1 provides the format for pricing TUCs for CSVS. Table B.2.2.2.4.2 provides CSVS TUC pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.2.2.4.1 CSVS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.2.2.4.2 CSVS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
VS99990	VS99991	VS99992	CSVS Task Order Unique	ICB	ICB

B.2.2.3 Toll Free Service

The technical requirements for Toll-Free Service (TFS) are defined in Section C.2.2.3. Note that TFS is for inbound calls only.

B.2.2.3.1 TFS Price Structure

TFS access may be 1) switched (i.e., off-net switched access, or switched access with pre- subscription to the contractor designated as on-net switched access), 2) dedicated, or 3) IP termination. TFS pricing does not include a separate price element for switched access. For calls originated over a switched access arrangement, the originating and terminating access costs shall be included in the transport pricing. For calls originated over a dedicated access arrangement, the dedicated access costs are not included in TFS pricing and are not covered in this section. Where dedicated access is used to connect the SDP to the contractor's designated connecting POP, dedicated access prices shall be provided in accordance with Section B.2.9. Prices for any associated SRE shall be provided in accordance with Section B.2.10.

B.2.2.3.1.1 Mandatory Price Structure

The mandatory price structure for TFS includes the following elements:

1. Transport usage (includes switched originating access cost, and/or terminating access costs, as applicable) per six-second increment
2. Payphone surcharge per call
3. Feature charges

Transport prices shall be usage-based in six-second increments. The following types of calls are differentiated:

1. Domestic to domestic
2. Non-domestic to domestic

The minimum required number of six-second billing increments per initial period for all calls is defined below in Table B.2.2.3.1.1.1. These minimum billing increments apply to all usage-based billing associated with a TFS call.

B.2.2.3.1.1.1 Minimum Billing Increments for Usage-Based Billing

From	To	Minimum Increments Per Call
Domestic	Domestic	One
Non-domestic	Domestic	Five

Any charges for dedicated access arrangements shall not be included in TFS pricing, but shall be provided as described in Section B.2.9.

B.2.2.3.1.2 Optional Price Structure

The TFS optional price structure shall either use pricing element (1) below, or both pricing elements (1) and (2):

1. Flat monthly rate for transport usage (includes a pre-determined number of maximum allowable minutes per month).
2. Transport usage per additional six-second increment for minutes of use above the maximum allowed per month.

If offered, flat rate pricing shall be provided on a per SDP basis, for calls between locations in CONUS, Alaska, and Hawaii; other OCONUS and non-domestic usage shall be charged as shown in Section B.2.2.3.3.3, and features as shown in Section B.2.2.3.4.

B.2.2.3.2 TFS Access Prices

Originating switched access costs for TFS shall be included in transport prices found in Section B.2.2.3.3. Charges for dedicated access arrangements shall be provided as described in Section B.2.9.

B.2.2.3.3 TFS Transport Prices

Tables B.2.2.3.3.1.1 through B.2.2.3.3.3.1 define the format for transport pricing information for TFS domestic and non-domestic connections. All TFS transport prices shall be billed in six-second increments unless otherwise offered optionally. A minimum number of billing increments per call for transport shall be set at the levels defined in Table B.2.2.3.1.1.1.

B.2.2.3.3.1 Mandatory Price Structure

Table B.2.2.3.3.1.1 provides the formats for pricing information for TFS domestic usage prices. Table B.2.2.3.3.1.2 provides applicable charging mechanisms and charging units for TFS domestic usage prices.

B.2.2.3.3.1.1 TFS Domestic Usage Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.2.3.3.1.2 TFS Transport Pricing Instructions Table

Usage CLIN	Description	Charging Unit
TF04001	TFS Transport Usage – Switched access termination	6 seconds
TF04002	TFS Transport Usage – Dedicated access termination	6 seconds
TF04003	TFS Transport Usage – IP access termination	6 seconds

Table B.2.2.3.3.1.3 provides the formats for pricing information for domestic payphone surcharge prices. Table B.2.2.3.3.1.4 provides applicable charging mechanisms and charging units for domestic payphone surcharge prices. The payphone surcharge shall apply only to 800 calls originated from a payphone.

B.2.2.3.3.1.3 Domestic Payphone Surcharge Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.2.3.3.1.4 Domestic Payphone Surcharge Pricing Instructions Table

Usage CLIN	Description	Charging Unit
TF04051	Payphone Surcharge	call

B.2.2.3.3.2 Optional Price Structure

Table B.2.2.3.3.2.1 provides the formats for pricing information for TFS CONUS, Alaska, and Hawaii flat rate prices. Table B.2.2.3.3.2.2 provides applicable charging mechanisms and charging units for TFS CONUS, Alaska, and Hawaii flat rate prices.

B.2.2.3.3.2.1 TFS CONUS, Alaska, and Hawaii Flat Rate Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.2.3.3.2.2 TFS CONUS, Alaska, and Hawaii Flat Rate Pricing Instructions Table

MRC CLIN	Description	Charging Unit	Notes
TF04201	TFS Flat Rate: Switched access termination up to TBD minutes	Month	ICB
TF04202	TFS Flat Rate: Dedicated access termination up to TBD minutes	Month	ICB
TF04203	TFS Flat Rate: IP access termination up to TBD minutes	Month	ICB

Overage charges shall be applied for minutes exceeding the maximum allowed per month. Table B.2.2.3.3.2.3 provides the formats for pricing information for TFS usage overage charges. Table B.2.2.3.3.2.4 provides applicable charging mechanisms and charging units for TFS usage overage charges.

B.2.2.3.3.2.3 TFS CONUS, Alaska, and Hawaii Overage Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.2.3.3.2.4 TFS CONUS, Alaska, and Hawaii Overage Pricing Instructions Table

~~MRC~~ Usage CLIN	Description	Charging Unit	Notes
TF04401	TFS Overage: Switched access termination over TBD minutes	6 seconds	ICB
TF04402	TFS Overage: Dedicated access termination over TBD minutes	6 seconds	ICB
TF04403	TFS Overage: IP access termination over TBD minutes	6 seconds	ICB

B.2.2.3.3.3 Non-Domestic Price Structure

Table B.2.2.3.3.3.1 provides the formats for pricing information for TFS non-domestic usage prices. Table B.2.2.3.3.1.2 provides the applicable charging mechanisms and charging units for TFS non-domestic transport prices.

B.2.2.3.3.3.1 TFS Non-Domestic to Domestic Transport Prices Table

CLIN	Task Order Number	Originating Country / Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* See Table B.4.2.1 for Country/Jurisdiction IDs

B.2.2.3.4 TFS Features

Table B.2.2.3.4.1 provides the formats for pricing information for TFS features. Table B.2.2.3.4.2 provides applicable charging mechanisms and charging units for TFS features.

Where features are offered non-domestically, the following pricing rules shall apply:

1. For features where normal call charges (basic service charges) also apply, the price applicable to the called country/jurisdiction (as determined by the called number) shall be used.
2. For features where normal call charges (basic service charges) do not apply, the price applicable to the calling country/jurisdiction shall be used (e.g., if locator service is offered in a specific country/jurisdiction, then the per-call price for that country/jurisdiction shall be used).

B.2.2.3.4.1 TFS Feature Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

** Applies only to ICB CLINs

B.2.2.3.4.2 TFS Feature Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
TF90001	TF90101		Agency-Based Routing Database (Host Connect)	Arrangement	
		TF90201	Agency-Based Routing Database (Host Connect)	Database Lookup	
		TF90202	Alternate Routing (Cascade Routing)	Each	NSP
TF90003	TF90103		ANI (Automatic Number Identification)	Number	NSP
		TF90204	ANI Based Routing	Each	

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
TF90005	TF90105		Announced Connect	Number	
TF90006	TF90106		Announcements (English/Spanish)	Announcement	NRC is initiation/change charge
TF90007	TF90107		Announcements (Other Languages)	Announcement	Optional. NRC is initiation/change charge.
		TF90208	Announcements (Initial 30 seconds played)	Announcement played initial 30 seconds	
		TF90209	Announcements (Each additional 6 seconds played)	Announcement played each additional 6 seconds	
TF90010	TF90110		Menu Routing (English/Spanish)	Announcement	Does not apply to generic (pre-recorded) announcements
TF90011	TF90111		Menu Routing (Other Languages)	Announcement	Optional
		TF90212	Menu Routing (Initial 30 seconds played)	Announcement played initial 30 seconds	
		TF90213	Menu Routing (Each additional 6 seconds played)	Announcement played each additional 6 seconds	
TF90014	TF90114		Call Redirection (Toll-Free Number)	Number	NRC is initiation/change charge
		TF90215	Call Redirection (Blind transfer)	Call	Normal TFS charges apply to a call redirected to a Toll Free number
		TF90216	Call Redirection (Verified not-busy or conference call transfer)	Call	Normal TFS charges apply to a call redirected to a Toll Free number
	TF90117		Call Redirection (Toll-Free Number Speed Dial Storage)	Number	

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
TF90018	TF90118		Computer Telephony Integration (CTI) - Application	Application	ICB
TF90019			Computer Telephony Integration (CTI) - Change	Change	ICB
	TF90120		Custom Call Records	Report	Charge applies to reports based on predefined record content
		TF90021	Custom Call Records	Minute	
TF90022			Day of Week Routing	Each	NSP
TF90023			Day of Year Routing (Holiday Routing)	Each	NSP
TF90024	TF90124		In Route Announcements (English/Spanish)	Announcement	Does not apply to generic (pre-recorded) announcements
TF90025	TF90125		In Route Announcements (Other Languages)	Announcement	Optional. Does not apply to generic (pre-recorded) announcements
		TF90226	In Route Announcements (Initial 30 Seconds)	Announcement Played initial 30 seconds	
		TF90227	In Route Announcements (Each Additional 6 Seconds)	Announcement Played additional 6 seconds	
TF90028			Vanity Toll Free Number	Number	Optional, NSP. The contractor shall provide agency-requested "vanity" toll-free numbers (e.g., 1-800-CALL-GSA), if available.
TF90031			Interactive Voice Response (IVR) Dedicated or Shared	Application	ICB
	TF90132		Interactive Voice Response (IVR) Dedicated	Port	
		TF90232	Interactive Voice Response (IVR) Shared	6 seconds	

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
	TF90138		Language Interpretation Service (Spanish)	Month	
		TF90239	Language Interpretation Service (Spanish)	Minute	
	TF90140		Language Interpretation Service (Other Languages)	Month	Optional, ICB
		TF90241	Language Interpretation Service (Other Languages)	Minute	Optional, ICB
TF90042			Make Busy Arrangement	Each	NSP. For use with dedicated access facilities only
TF90043	TF90143		Network Call Distributor – Host-based	Concurrent user	ICB. The concurrent user count for pricing is the maximum number of simultaneous users.
TF90044	TF90144		Network Call Distributor – Premises-based	Concurrent user	ICB. The concurrent user count for pricing is the maximum number of simultaneous users
TF90045			Network Queuing - Per Toll Free Number	Service Initiation	Optional
	TF90146		Network Queuing - Per Toll Free Number	Number	Optional
		TF90247	Network Queuing - Per Toll Free Number	6 seconds	Optional
TF90048			NPA/NXX Routing	Each	NSP
TF90049	TF90149		Office Locator Database	Application	NRC is initiation charge
TF90050			Office Locator Database Service Change	Application	
TF90053			Percentage Call Allocation	Each	NSP
TF90054			Real Time Reporting	Each	
	TF90155		Real Time reporting, unlimited access	Month	

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
		TF90256	Routing Control (Initial hour)	Initial hour or fraction thereof for terminal connect time in a billing month	
		TF90257	Routing Control (Additional minutes)	Additional minute of terminal connect time in a billing month	
TF90058	TF90158		Service Assurance Routing	Arrangement	NRC is initiation charge
TF90059			Speech Recognition - Shared or Dedicated	Application	ICB
		TF90260	Speech Recognition - Shared	6 seconds	
		TF90261	Speech Recognition - Dedicated	Port	
TF90062			Tailored Call Coverage per Toll-Free Number	Number	
	TF90163		Tailored Call Coverage per Toll-Free Number	Number	
TF90064			Time of Day Routing	Each	NSP
TF90065			Virtual Call Queue	Service Initiation	
	TF90166		Virtual Call Queue	Arrangement	ICB
		TF90267	Virtual Call Queue	Call	
TF90069	TF90169		Enhanced Transfer	Arrangement	
		TF90270	Blind Transfer	Transfer	Requires Enhanced Transfer arrangement
		TF90271	Supervised Transfer	Transfer	Requires Enhanced Transfer arrangement
		TF90272	Conference Transfer	Transfer	Requires Enhanced Transfer arrangement
TFS Features: Reports					

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
TF99001	TF99101		Call Status Report – Toll-Free Service	Report	
TF99002	TF99102		Call Status Report – Alternate Routing	Report	
TF99003	TF99103		Call Status Report – Announcement	Report	
TF99004	TF99104		Call Status Report – Call Prompter	Report	
TF99005	TF99105		Call Status Report – IVR	Report	
TF99006	TF99106		Caller Information Report	Report	
TF99007	TF99107		Caller Profile Report	Report	
TF99008	TF99108		Call Redirection Report	Report	Optional
TF99209			Custom Reporting	Report	ICB

B.2.2.3.5 TFS Task Order Unique CLINs

Table B.2.2.3.5.1 provides the format for pricing TUCs supported by TFS. Table B.2.2.3.5.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.2.3.5.1 TFS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.2.3.5.2 TFS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
TF99990	TF99991	TF99992	TFS Task Order Unique	ICB	ICB

B.2.2.4 Circuit Switched Data Service

The technical requirements for Circuit Switched Data Service (CSDS) are defined in Section C.2.2.4.

B.2.2.4.1 Circuit Switched Data Service Price Structure

CSDS data calls shall be priced based on one or more of three components: 1) originating access, 2) transport, and 3) features. Originating access may be switched (i.e., off-net switched access or switched access with pre-subscription to contractor, designated as on-net switched access) or dedicated. For calls originated over a switched access arrangement, the originating and terminating access costs shall be included in the transport pricing. For calls originating over a dedicated access arrangement, the dedicated access costs are not included in CSDS pricing and are not covered in this section. Price tables for dedicated access arrangements are located in Section B.2.9.

Any SRE required for the contractor's provision of CSDS dedicated access is located in Section B.2.10. All other CSDS-related price tables are located in this section. With the exception of any dedicated access costs at the call terminating location, all other terminating access costs shall be included in the transport pricing. Transport prices shall be usage-based in six-second increments.

The minimum required initial billing period for all calls shall not exceed the number of six-second increments shown in Table B.2.2.4.1.1. This applies to all usage-based billing associated with a CSDS call.

B.2.2.4.1.1 Minimum Billing Increments for Usage-Based Billing on Circuit Switched Data Service Calls Table

From	To	Minimum Increments for Initial Period
Domestic	Domestic	1
Domestic	Non-domestic	3
Non-domestic	Domestic, Non-domestic	5

B.2.2.4.1.2 CONUS to CONUS Circuit Switched Data Service Pricing Components

For all CONUS to CONUS calls (i.e., calls that originate and terminate at CONUS locations) two different call types shall be priced: 1) for calls using switched originating access and 2) for calls using dedicated originating access. Each call type shall be postalized across all CONUS locations, and shall not include a time-of-day price differential.

B.2.2.4.1.3 OCONUS and Non-Domestic Circuit Switched Data Service Pricing Components

B.2.2.4.1.3.1 CONUS to OCONUS and Non-Domestic Calls

The basic service price for CSDS connections that originate from a CONUS location at one end and terminate at a OCONUS or non-domestic location at the other shall be priced on a basis similar to CONUS calls (i.e., two different call types shall be priced per terminating non-CONUS country/jurisdiction): 1) pricing for calls using switched originating access, and 2) pricing for calls using dedicated originating access.

Switched originating access costs shall be included in the transport pricing; dedicated originating access costs are not included in CSDS pricing and are not covered in this section. Price tables for dedicated access and any associated SRE are located in Sections B.2.9 and B.2.10. All other terminating access costs shall be included in the transport pricing. Transport prices shall be usage-based in six-second increments, with per-call minimum increments as defined in Table B.2.2.4.1.1. Pricing shall be provided on a per-termination country/jurisdiction basis. No time-of-day pricing differential shall be permitted.

B.2.2.4.1.3.2 OCONUS or Non-Domestic to CONUS Calls

The basic service price for CSDS connections that originate from an OCONUS or non-domestic location at one end and terminate at a CONUS location at the other shall be priced on a basis similar to CONUS to CONUS calls, i.e., two different call types shall be priced per-originating OCONUS or non-domestic country/jurisdiction: 1) pricing for calls using switched originating access and 2) pricing for calls using dedicated originating access. Pricing shall be provided on a per-originating country/jurisdiction basis. No time-of-day pricing differential shall be permitted. Switched originating access costs shall be included in the transport pricing. Dedicated originating access costs are not included in CSDS pricing and are not covered in this section. Any charges for domestic dedicated access arrangements at the terminating location are not included in the CSDS pricing. All other originating and terminating access costs shall be included in the transport pricing. Transport prices shall be usage-based in six-second increments, with per-call minimum increments as defined in Table B.2.2.4.1.1.

Pricing shall be provided on a per-originating country/jurisdiction basis. No time-of-day pricing differential shall be permitted.

B.2.2.4.1.3.3 OCONUS or Non-Domestic to OCONUS or Non-Domestic Calls

The basic service price for CSDS connections that originate from an OCONUS or non-domestic location at one end and terminate at an OCONUS or non-domestic location at the other shall be priced on a basis similar to CONUS to CONUS calls, i.e., two

different call types shall be priced per-originating OCONUS or non-domestic country/jurisdiction: 1) pricing for calls using switched originating access and 2) pricing for calls using dedicated originating access. Switched originating access costs shall be included in the transport pricing; dedicated originating access costs are not included in CSDS pricing and are not covered in this section. Any charges for OCONUS or non-domestic dedicated access arrangements at the terminating location are not included in the CSDS pricing. All other originating and terminating access costs shall be included in the transport pricing. Transport prices shall be usage-based in six-second increments, with per call minimum increments as defined in Table B.2.2.4.1.1.

Transport pricing shall be listed on a country/jurisdiction-to-country/jurisdiction basis between the countries/jurisdictions involved in the call. No time-of-day pricing differential shall be permitted.

B.2.2.4.2 Circuit Switched Data Service Access Prices

Originating and/or terminating switched access costs for CSDS shall be included in transport prices found in Section B.2.2.4.3. Pricing for a domestic dedicated access arrangement connection to the CSDS transport network may be provided in Section B.2.9. No separate CSDS pricing shall be permitted for terminating access.

B.2.2.4.3 Circuit Switched Data Service Transport Prices

Tables B.2.2.4.3.2 through Table B.2.2.4.3.5 define the formats for transport pricing information for CSDS domestic and non-domestic connections. Pricing instructions are provided in B.2.2.4.3.6. All CSDS transport prices shall be billed in six-second increments. A minimum number of billing increments per call for transport shall be set at the levels defined in Table B.2.2.4.1.1~~B.2.2.4.1.1~~. The pricing tables applicable to all categories of OCONUS or non-domestic transport (outbound, inbound, and OCONUS or non-domestic to OCONUS or non-domestic) are listed in Table B.2.2.4.3.1~~B.2.2.4.3.1~~.

Formatte

Formatte

B.2.2.4.3.1 *OCONUS and Non-Domestic Transport Category Price Table Cross-Reference*

From Location	To Location	Table
CONUS	CONUS	B.2.2.4.3.2
CONUS	OCONUS or Non-Domestic	B.2.2.4.3.3~~B.2.2.4.3.3~~
OCONUS or Non- Domestic	CONUS	B.2.2.4.3.4~~B.2.2.4.3.4~~

Formatte

Formatte

From Location	To Location	Table
OCONUS or Non- Domestic	OCONUS or Non-Domestic	B.2.2.4.3.5~~B.2.2.4.3.5~~

Formatte

CONUS CSDS usage pricing shall be based on a fixed per six-second charge for all local toll and long distance calls.

B.2.2.4.3.2 Circuit Switched Data Service CONUS Transport Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.2.4.3.3 Circuit Switched Data Service CONUS to OCONUS or Non-Domestic Transport Prices Table

CLIN	Task Order Number	Terminating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.4.3.4 Circuit Switched Data Service OCONUS or Non-Domestic to CONUS Transport Prices Table

CLIN	Task Order Number	Originating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.4.3.5 Circuit Switched Data Service OCONUS or Non-Domestic to OCONUS or Non-Domestic Transport Prices Table

CLIN	Task Order Number	Originating Country/ Jurisdiction ID*	Terminating Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.2.4.3.6 Circuit Switched Data Service Transport Pricing Instructions Table

Usage CLIN	Description	Charging Unit
CS20001	Switched Access, DS0 origination	6 second increment
CS20101	Dedicated Access, DS0 origination	6 second increment

B.2.2.4.4 Circuit Switched Data Service Task Order Unique CLINs

Table B.2.2.4.4.1 provides the format for pricing CSDS TUCs. Table B.2.2.4.4.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.2.4.4.1 Circuit Switched Data Service TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.2.4.4.2 Circuit Switched Data Service TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
CS99990	CS99991	CS99992	CSDS Task Order Unique	ICB	ICB

B.2.3 Contact Center Service

The technical requirements for Contact Center Service (CCS) are defined in Section C.2.3.

B.2.3.1 CCS Price Structure

The mandatory price structure for CCS varies by type of service and includes the following elements:

1. NRC for one-time service initiation charge
2. NRC based on the number of concurrent agents
3. MRC based on the number of concurrent agents
4. Feature Charges (composed of NRC, MRC, and/or Usage Charges)

Pricing for access and transport required to connect to the contractor's network shall not be included in CCS pricing.

The contractor shall use the SRE Catalog pricing for all necessary equipment described in Section B.2.10, including terminal devices and software for CCS.

B.2.3.2 CCS Basic Service Prices

CCS basic service shall apply only to inbound voice calls, and shall exclude network connectivity services (e.g., PSTN and data network connectivity services). Additional components, such as Interactive Voice Response (IVR), email, text chat (web chat), and web collaboration, shall be priced as CCS features.

A terminal device is a phone, IP phone or soft phone that is installed and configured in the contact center. An IVR shall not be considered as a terminal device. An agent is a call answering resource that is logged into the call routing system (e.g., the ACD) at the same time as other call answering resources. The number of concurrent agents is always less than or equal to the number of terminal devices and equates to the maximum number of simultaneous agents.

For all the CCS delivery methods, the contractor shall provide an ICB NRC for a one-time service initiation charge that includes system design and integration and software development.

For the Premises-based CCS delivery method only, this ICB NRC shall additionally include the initial installation of any routing and distribution equipment. The contractor shall charge an NRC for each terminal device as defined in the SRE Catalog in Section B.2.10, and an NRC for each concurrent user.

For Premises-based, the contractor shall provide two types of NRCs for active agents:

1. Initial provisioning
2. Incremental provisioning

Premises-based NRCs for initial provisioning shall be determined from the corresponding volume range containing the number of active agents requested in the initial order. Premises-based NRCs for incremental provisioning have no volume bands.

The contractor shall also provide a Premises-based MRC for each active agent. For each contact center, the contractor shall determine the MRCs for each month from the corresponding volume range that contains the maximum number of active agents for that month.

Host-based NRCs will be used by agencies for both the initial and incremental (or subsequent) provisioning of terminal devices and concurrent users for their contact center. The Host-based NRC shall be determined from the corresponding volume range containing the number of concurrent users (active agents) in that order.

The contractor shall also provide a Host-based MRC for each terminal device as defined in the SRE Catalog in Section B.2.10 and an MRC for each active agent. For

each contact center, the contractor shall determine the MRCs for each month from the corresponding volume range that contains the maximum number of active agents for that month.

Basic and Advanced Call Answering Service shall be priced as ICBs for both Premises-based and Host-based CCS services as appropriate.

B.2.3.2.1 Host-Based Call Management Service

Tables B.2.3.2.1.1 and B.2.3.2.1.2 provide the formats for pricing information for Host-based CCS. Tables B.2.3.2.1.3 and B.2.3.2.1.4 provide applicable charging mechanisms and charging units for Host-based CCS.

B.2.3.2.1.1 Host-Based Service Initiation Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.3.2.1.2 Host-Based Active Agents Prices Table

CLIN	Task Order Number	Band Low	Band High	Variable Price	Price Start Date	Price Stop Date

B.2.3.2.1.3 Host-Based Service Initiation Pricing Instructions Table

NRC CLIN	Description	Charging Unit	Notes
CC00001	Host-Based Service Initiation Charge	Service Initiation	ICB

B.2.3.2.1.4 Host-Based Active Agents Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit
CC00002	CC00102	Host-Based Call Management Active Agents	Active Agent

B.2.3.2.2 Premises-Based Call Management Service

Tables B.2.3.2.2.1 and B.2.3.2.2.2 provide the formats for pricing information for Premises-based CCS. Tables B.2.3.2.2.3 through B.2.3.2.2.5 provide applicable charging mechanisms and charging units for Premises-based CCS.

B.2.3.2.2.1 Premises-Based Service Initiation Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.3.2.2.2 Premises-Based Active Agents Prices Table

CLIN	Task Order Number	Band Low	Band High	Variable Price	Price Start Date	Price Stop Date

B.2.3.2.2.3 Premises-Based Service Initiation Pricing Instructions Table

NRC CLIN	Description	Charging Unit	Notes
CC00020	Premises-Based Service Initiation Charge	Service Initiation	ICB

B.2.3.2.2.4 Premises-Based Active Agents Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit
CC00021	CC00121	Premises-Based Call Management Active Agents	Active Agent

B.2.3.2.2.5 NRC for Incremental Premises-Based Active Agents Pricing Instructions Table

NRC CLIN	Description	Charging Unit
CC00030	Incremental Premises-Based Active Agents	Active Agent

B.2.3.2.3 CCS Call Answering Service

There are two CCS Call Answering Service types: 1) Premises-based and 2) Host-based. Host-based CCS has two types of call answering: 1) Basic Call Answering, and 2) Advanced Call Answering. Table B.2.3.2.3.1 provides the Premises-based and Host-based pricing information formats. Table B.2.3.2.3.2 provides the applicable charging mechanisms and charging units for Basic and Advanced Call Answering Service, which shall consist of the labor rates for various categories provided in Section B.2.11.

B.2.3.2.3.1 CCS Call Answering Service Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.3.2.3.2 CCS Call Answering Service Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
CC00050	CC00150	Premises-Based – Call Answering Service	Service initiation; Month	ICB
CC00051	CC00151	Host-Based – Call Answering Service	Service initiation; Month	ICB

B.2.3.2.4 CCS Feature Prices

Table B.2.3.2.4.1 provides the formats for pricing information for CCS features. Table B.2.3.2.4.2 and Table B.2.3.2.4.3 provide applicable charging mechanisms and charging units for the Host-based and Premises-based CCS features, respectively. Each feature table identifies all of the features that apply to a particular service delivery method. Table B.2.3.2.4.2~~B.2.3.2.4.2~~ provides the list of features that apply to Host-based CCS, and Table B.2.3.2.4.3 provides features that apply to Premises-based CCS. Since some features apply to more than one service delivery method, some feature CLINs appear in more than one pricing instructions table.

Formatte

Each CLIN may have only one price in Table B.2.3.2.4.1 for a given date range. The Charging Unit column defines the charging unit, identifies the ICB CLINs, and identifies CLINs that are one-time charges at service initiation with the phrase “service initiation charge.” For the features with ICB NRCs, the contractor shall include application development in the NRCs. Custom Reporting is provided as an ICB feature CLIN.

Scheduled call answering resources are defined as the number of resources that will be managed using the Workforce Management feature.

Prices for the transcription requirements listed in the description of the IVR feature (Section C.2.2.3.2 Features, item #14) may be found in Section B.2.2.3.4 (TFS Features) with the pricing for the Call Prompter feature.

Usage CLINs have charging units of six-second increments.

B.2.3.2.4.1 CCS Feature Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.3.2.4.2 Host-Based CCS Feature Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
CC90001	CC90101		Call Recording and Monitoring – Host-Based	Service initiation; Month	ICB
CC90002	CC90102		Collaborative Browsing – Host-Based	Active agent	
CC90003	CC90103		CTI – Host-Based	Service initiation; Month	ICB
CC90004	CC90104		Customer Contact Application – Host-Based	Service initiation; active agent	ICB
CC90005	CC90105		Email Response Management – Host-Based	Active agent	
CC90006		CC90206	IVR – Shared	Service initiation; 6 seconds	ICB
CC90007		CC90207	IVR – Speech Recognition – Shared	Service initiation; 6 seconds	ICB
CC90008	CC90108		IVR – Agency Based Database (Host Connect) – Host-Based	Service initiation; port	ICB
CC90011			Language Interpretation Service – Host-Based	Service initiation	
		CC90212	Spanish Language Interpretation Service (DNBH*) – Host-Based	6 seconds	
		CC90213	Spanish Language Interpretation Service (ONBH**) – Host-Based	6 seconds	
		CC90214	Other Language Interpretation Service (DNBH*) – Host-Based	6 seconds	Optional, ICB
		CC90215	Other Language Interpretation Service (ONBH**) – Host-Based	6 seconds	Optional, ICB
CC90016			Outbound Dialer – Host-Based	Instance	

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
CC90017			Text Chat (Web Chat) – Host-Based	Instance	
CC90018			Web Call Back – Host-Based	Service initiation	
CC90019			Web Call Through – Host-Based	Service initiation	
CC90020	CC90120		Workforce Management – Host-Based	Scheduled call answering resource	
CC90021	CC90121		Knowledge Management – Host-Based	Each	ICB
CC90022	CC90122		Custom Reporting – Host-Based	Report	ICB
CC90023	CC90123	CC90223	Virtual Call Queue – Host-Based	Service initiation; Arrangement; Call	MRC is ICB

* DNBH = During Normal Business Hours (8:00 a.m. to 5:00 p.m. Monday through Friday Eastern Time)
** ONBH = Outside Normal Business Hours (5:01 p.m. to 7:59 a.m. Monday through Friday and all day Saturday and Sunday Eastern Time)

B.2.3.2.4.3 Premises-Based CCS Feature Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
CC92001	CC92101		Call Recording and Monitoring – Premises-Based	Service initiation; Month	ICB
CC92002	CC92102		Collaborative Browsing – Premises-Based	Active agent	
CC92003	CC92103		Computer Telephony Integration (CTI) – Premises-Based	Service initiation; Month	ICB
CC92004	CC92104		Customer Contact Application – Premises-Based	Service initiation; Active agent	ICB
CC92005	CC92105		E Mail Response Management – Premises-Based	Active agent	
CC92006	CC92106		Interactive Voice Response (IVR) – Dedicated	Service initiation; Port	ICB
CC92007	CC92107		IVR – Speech Recognition – Dedicated	Service initiation; Port	ICB
CC92008	CC92108		IVR – Agency Based Database (Host Connect) – Premises-Based	Service initiation; port	ICB

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
CC92011			Language Interpretation Service – Premises-Based	Service initiation	
		CC92212	Spanish Language Interpretation Service (DNBH*) – Premises-Based	6 seconds	
		CC92213	Spanish Language Interpretation Service (ONBH**) – Premises-Based	6 seconds	
		CC92214	Other Language Interpretation Service (DNBH*) – Premises-Based	6 seconds	Optional, ICB
		CC92215	Other Language Interpretation Service (ONBH**) – Premises-Based	6 seconds	Optional, ICB
CC92016			Outbound Dialer – Premises-Based	Instance	
CC92017			Text Chat (Web Chat) – Premises-Based	Instance	
CC92018			Web Call Back – Premises – Based	Service initiation	
CC92019			Web Call Through – Premises-Based	Service initiation	
CC92020	CC92120		Workforce Management – Premises-Based	Scheduled call answering resource	
CC92021	CC92121		Knowledge Management – Premises-Based	Each	ICB
CC92022	CC92122		Custom Reporting – Premises-Based	Report	ICB
CC92023	CC92123	CC92223	Virtual Call Queue – Premises-Based	Service initiation; Arrangement; Call	MRC is ICB

* DNBH = During Normal Business Hours (8:00 a.m. to 5:00 p.m. Monday through Friday Eastern Time)
** ONBH = Outside Normal Business Hours (5:01 p.m. to 7:59 a.m. Monday through Friday and all day Saturday and Sunday Eastern Time)

B.2.3.3 CCS Task Order Unique CLINs

Table B.2.3.3.1 provides the format for pricing TUCs supported by CCS. Table B.2.3.3.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.3.3.1 CCS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.3.3.2 CCS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
CC99990	CC99991	CC99992	CCS Task Order Unique	ICB	ICB

B.2.4 Colocated Hosting Service

The technical requirements for Colocated Hosting Service (CHS) are defined in Section C.2.4.

B.2.4.1 CHS Price Structure

The price structure for CHS includes the following elements:

1. NRC
2. MRC
3. Usage charges for additional bandwidth
4. Feature Charges

When access is required or requested by the customer, then the access prices in Section B.2.9 shall be used.

Prices for any associated SRE shall be provided in accordance with Section B.2.10.

B.2.4.2 CHS Basic Service Prices

The prices for CHS are applicable to all domestic locations. The contractor shall charge a monthly recurring charge for rack space (see Section C.2.4.1). This charge shall include all elements necessary to provide the services, such as building/facilities, power systems, fire suppression, cooling systems and security. The full rack space monthly price includes basic power options of 110V/208V/220V/240V, 20A/30A, single phase/three phase, as required. Non-basic power is ICB. Internet connectivity bandwidth to the government applications servers on the contractors' racks is priced separately. The contractor may charge an NRC for installation or initiation of service.

The monthly Internet usage shall be determined by the 95th percentile method, where the usage shall be measured daily every five minutes. The top 5% of monthly usage shall be discarded and the maximum usage remaining, representing the 95th percentile, shall be designated as the Internet usage amount for the month.

Table B.2.4.2.1 provides the format for pricing information for CHS. Instruction tables B.2.4.2.2 and B.2.4.2.3 provide the pricing information and charging units for CHS. The monthly Internet usage charge shall be based on the usage bands identified in Instruction table B.2.4.2.3. The customer may purchase SRE, such as a server or group of servers, from the SRE Catalog (see Section B.2.10).

B.2.4.2.1 CHS Basic Service Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Used for Individual Case Basis (ICB) priced items

B.2.4.2.2 CHS Pricing Instructions Table – Rack Space

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
CH11003	CH12003		Full Rack Space*	Full Rack	6 shelves (72” x 19” x 32”). CH12003 Includes basic power.
CH11004	CH12004		Custom Colocation Center Build-out and Support	ICB	ICB
CH11005		CH13005	Non-Basic Power	ICB	ICB
CH11006	CH12006		Cross Connect (Twisted Pair)	Connection	
CH11007	CH12007		Cross Connect (Coax Cable)	Connection	
CH11008	CH12008		Cross Connect (Fiber)	Connection	
CH11009	CH12009		SCIF	Connection	ICB

* See Electronic Industry Association (EIA)-310 for rack space specifications

B.2.4.2.3 CHS Pricing Instructions Table – Internet Bandwidth Usage

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
CH21002	CH22002		Dedicated burstable Internet bandwidth – maximum 10 Mbps, initial 1 Mbps	Connection	Requires CH23002

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
		CH23002	Dedicated burstable Internet bandwidth – usage above 1 Mbps up to and including 10 Mbps	1 Mbps	Requires CH21002 and CH22002
CH21003	CH22003		Dedicated burstable Internet bandwidth – maximum 100 Mbps, initial 10 Mbps	Connection	Requires CH23003
		CH23003	Dedicated burstable Internet bandwidth – usage above 10 Mbps up to and including 100 Mbps	10 Mbps	Requires CH21003 and CH22003
CH21004	CH22004		Dedicated burstable Internet bandwidth – maximum 1 Gbps, initial 100 Mbps	Connection	Requires CH23004
		CH23004	Dedicated burstable Internet bandwidth – usage above 100 Mbps up to and including 1 Gbps	100 Mbps	Requires CH21004 and CH22004
CH21005	CH22005		Dedicated burstable Internet bandwidth – maximum 10 Gbps, initial 1 Gbps	Connection	Optional. Requires CH23005
		CH23005	Dedicated burstable Internet bandwidth – usage above 1 Gbps up to and including 10 Gbps	1 Gbps	Optional. Requires CH21005 and CH22005
CH21006	CH22006		Specialized Dedicated Burstable Internet Bandwidth	Connection	ICB

B.2.4.3 CHS Feature Prices

Table B.2.4.3.1 provides the format for pricing the features supported by CHS. Instruction table B.2.4.3.2 provides the pricing information and charging unit. Note that those features that are not separately priced are identified by the term “NSP” in their price column.

B.2.4.3.1 CHS Feature Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.4.3.2 CHS Feature Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
CH32001	CH31001	Basic Subscriber Line	Line	
CH32002	CH31002	Cabinets	Cabinet	ICB
CH32003	CH31003	Cages	Cage	ICB
CH32004	CH31004	Host Administrative Tasks	Server	On behalf of the agency, IDC staff shall intervene and perform minor unscheduled tasks including: 1. Rebooting of government-furnished equipment (limited to power cycling). 2. Manual entry of commands to servers from a keyboard. 3. Inspection and reading of alarm indicators and displays. 4. Securing cabling to connections. 5. Setting a dip switch. 6. Other minor tasks as appropriate.
	CH31010	Periodic Hardware Check (Ping)	Address	NSP
	CH31020	Reporting	Report	NSP. Price included in MRC (CH12003)

B.2.4.4 CHS Task Order Unique CLINs

Tables B.2.4.4.1 provides the format for pricing TUCs associated with CHS. Table B.2.4.4.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.4.4.1 CHS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.4.4.2 CHS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
CH99990	CH99991	CH99992	CHS Task Order Unique	ICB	ICB

B.2.5 Cloud Service

B.2.5.1 Cloud Service Price Structure

The government requires a catalog pricing approach for these cloud service types:

1. The technical requirements for Infrastructure as a Service (IaaS) are defined in Section C.2.5.1.
2. The technical requirements for Platform as a Service (PaaS) are described in Section C.2.5.2.
3. The technical requirements for Software as a Service (SaaS) are described in Section C.2.5.3.

B.2.5.2 Cloud Service Catalog Requirements for Pricing Information

Cloud services represent a wide array of services and service variations. Many providers offer permutations and combinations of a core set of services, as well as special tailored services. The needs of users may vary considerably. Accordingly, for pricing purposes, contractors shall provide a Cloud Service Catalog consistent with the service requirements found in C.2.5, and with the pricing catalog requirements found in Section B.1.3.

The Cloud Service Catalog provided by the contractor shall, at a minimum, contain the data elements defined in the tables below.

When Cloud Service offerings include equipment, all related equipment or equipment features shall be identified and priced in accordance with the SRE requirements in Section B.2.10.

When Cloud Service-related labor is offered, then labor rates shall be specified and priced in accordance with Section B.2.11.

Otherwise, Cloud Service prices for non-labor and non-SRE elements shall be determined from the catalog based on the information required as shown in Table B.2.5.2.1 below. The contractor shall identify the trade name(s) for the OLP. Charging mechanisms for the Cloud Service Catalog are provided in Table B.2.5.2.3.

Additional discounts or reduced prices may be negotiated at the time of TO award between the ordering agency and the contractor.

B.2.5.2.1 Cloud Service Catalog – Service Specification Table

CLIN	Case Number	Service Description*	Vendor Unique ID (e.g., SKU)**	OLP	No List Price***	Service Class ID	Start Date	Stop Date	End of Sale Date****	End of Life Date*****	Notes
						(from Table B.2.5.2.2~~B.2.5.2.2~~)					

Formatte

* Descriptions shall be sufficiently complete that all capabilities and limitations of the cloud service, as priced, are clear to the government
** Vendor Unique ID is any method of unambiguously identifying items in the catalog.
*** "T" if the price appearing in the OLP column is not an official list price, "F" otherwise
**** The End of Sale Date shall be the effective date after which an item may no longer be purchased. Stop Date shall not be later than End of Sale Date.
***** The End of Life Date shall be the effective date after which an item is no longer supported by the contractor

The discount to be applied to the OLP is determined by the Service Class, the elements of which are shown below in Table B.2.5.2.2. The Cloud Service NRC, MRC and/or Usage price shall be the OLP, less the discount for the service class. If no Official List Price exists, the contractor shall specify its price in the OLP column, populate the No List Price column with "T", and assign a Service Class ID where the discount is 0% (i.e., Service Class 1000).

B.2.5.2.2 Cloud Service Catalog – Service Class Discount Table

Service Class ID*	Service Class Description**	Task Order Number	Percentage Discount from OLP	Start Date	Stop Date
1000	Non-discounted		0		
1001					
…					
1999					

* The number of service classes shall be selected by the contractor from within the range shown
** The service class description and the percentage discount for each service class shall be constant and fixed through the life of the contract, unless changed by contract modification (the Start and Stop Dates shall only apply when a change is caused by contract modification).

The Service Class discount and catalog price shall not vary by geographic location.

B.2.5.2.3 Cloud Service Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
IA90001	NRC	IaaS Cloud Service Catalog Item	ICB	ICB
IA90002	MRC	IaaS Cloud Service Catalog Item	ICB	ICB
IA90003	Usage	IaaS Cloud Service Catalog Item	ICB	ICB
PA90001	NRC	PaaS Cloud Service Catalog Item	ICB	ICB
PA90002	MRC	PaaS Cloud Service Catalog Item	ICB	ICB
PA90003	Usage	PaaS Cloud Service Catalog Item	ICB	ICB
SS90001	NRC	SaaS Cloud Service Catalog Item	ICB	ICB
SS90002	MRC	SaaS Cloud Service Catalog Item	ICB	ICB
SS90003	Usage	SaaS Cloud Service Catalog Item	ICB	ICB

B.2.5.2.4 Cloud Service Task Order Unique CLINs

The tables below provide the format and instructions for pricing Cloud Service TUCs. TUCs shall be used as defined in Section B.1.2.15.

B.2.5.2.4.1 Cloud Service TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.5.2.4.2 Cloud Service TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
IA99990	IA99991	IA99992	IaaS Task Order Unique	ICB	ICB
PA99990	PA99991	PA99992	PaaS Task Order Unique	ICB	ICB
SS99990	SS99991	SS99992	SaaS Task Order Unique	ICB	ICB

B.2.5.3 Content Delivery Network Service

The technical requirements for Content Delivery Network Service (CDNS) are defined in Section C.2.5.4. CDNS data transfer pricing is based on the Content Delivery Network

(CDN) node location from where the transfers are served, not the end user's location. All transfers shall be serviced from a CONUS location.

B.2.5.3.1 CDNS Price Structure

CDNS shall be priced based on a banded price structure. Prices for a given usage level shall be calculated by summing the bands for all lesser usage bands times their unit price per band, and then adding the increment of usage above the band minimum within the band where the given usage falls times the band unit price. These prices shall not include the cost of reading data from storage and transferring data from storage to CDN.

The CDNS price table shall be completed using the contractor's banding structure. In order to correctly price the cumulative price bands, each band shall include a fixed price and a variable price component. Table B.2.5.3.1.1 provides the price table followed by an example of the banding structure.

B.2.5.3.1.1 CDNS Price Table

CLIN	Task Order Number	Band Low	Band High	Fixed Price Element	$/GB Variable Price Element	Price Start Date	Price Stop Date

Table B.2.5.3.1.1.1 provides a CDNS pricing example that includes 4 bands. Using Table B.2.5.3.1.1, the price (P) for a given amount of data transferred (T) shall be determined by the formula $P_n = F_n + (T-L_n)*V_n$ where n is the number of the price table row where T lies within the Band Low and Band High, according to the rules specified in Section B.1.2.4.

B.2.5.3.1.1.1 CDNS Pricing Example

CLIN	Task Order Number	Band Low	Band High	Fixed Price Element	$/GB Variable Price Element	Price Start Date	Price Stop Date
		$L_1=0$	H_1	$F_1=0$	V_1		
		L_2	H_2	$F_2=H_1*V_1$	V_2		
		L_3	H_3	$F_3=F_2+(H_2-H_1)*V_2$	V_3		
		L_4	H_4	$F_4=F_3+(H_3-H_2)*V_3$	V_4		

The contractor shall complete the CDNS price table using its banding structure. Table B.2.5.3.1.2 provides the applicable charging mechanisms and charging units.

B.2.5.3.1.2 CDNS Pricing Instructions Table

Usage CLIN	Description	Charging Unit
CD00100	CDNS Outbound Data	GB

B.2.5.3.2 CDNS Task Order Unique CLINs

The tables below provide the format and instructions for pricing CDNS TUCs. TUCs shall be used as defined in Section B.1.2.15.

B.2.5.3.2.1 CDNS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.5.3.2.2 CDNS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
CD99990	CD99991	CD99992	CDNS Task Order Unique	ICB	ICB

B.2.6 Wireless Service

The technical requirements for Wireless Service (MWS) are defined in Section C.2.6. These include services offered by the cellular industry.

The price structure for MWS includes the following elements:

1. NRC
2. MRC
3. Usage charges

All MRC prices are per device unless specified otherwise. Features are normally separately priced, although some features are defined as NSP. Domestic roaming fees and domestic roaming usage charges are not permitted. For MWS, domestic is defined as the contiguous United States, Alaska, Hawaii, Puerto Rico, and the U.S. Virgin Islands.

Bandwidth throttling (intentional slowing of data speeds by the service provider) is not permitted.

A contractor may prohibit unlimited data add-on or data only plans from being purchased for machine-to-machine (M2M) or similar types of applications (e.g., automated video feeds), or as a substitute for a private line or a dedicated data connection. In these cases, the customer may purchase a limited data add-on or data only plan or obtain an M2M plan.

Services may be suspended by a customer up to the maximum number of days allowed per 47 C.F.R. 52.15(f)(1)(vi) (180 days as of May 2015) without incurring any fees, subscription or usage charges during the suspension period.

B.2.6.1 Domestic Mobile Voice Service

The Domestic Mobile Voice Service listed below can be ordered as a standalone service or with Data Add-on Services.

B.2.6.1.1 Domestic Mobile Voice Service Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.6.1.2 Domestic Mobile Voice Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit
WL00001	MRC	Unlimited voice with unlimited SMS and MMS messaging services.	Line

B.2.6.2 Domestic Mobile Data Add-on Services

All Mobile Data Add-on Services (for smart phones) must be ordered with Voice Service. A personal hotspot shall be included at no additional cost with all Mobile Data Add-on Plans, except Unlimited Data.

The data allocations from all plans except Unlimited Data are pooled or added together across the agency(s) or entity(s) defined in the TO. Thus, if a 3 GB plan is ordered for one device and a 5 GB plan is ordered for another device, the pool of data that could be used between the two devices is 8 GB before any overages are paid. The contractor shall allocate overages only to those users who have exceeded their individual share of the pool, that is, without applying overage charges to any users who have not exceeded their own share. The data used for Personal Hotspots will be subtracted from the base

Data Add-on plan except in the case of when the Personal Hotspot feature is ordered with the Unlimited Data Add-on plan. In that case, the data used will be subtracted from the Personal Hotspot data allowance (5 GB minimum). Any Personal Hotspot overages may be billed via CLIN WL00020 Pooling Overage for Data Add-on.

B.2.6.2.1 Domestic Mobile Data Add-on Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.6.2.2 Domestic Mobile Data Add-on Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit
WL00010	MRC	1 GB Data Add-on Pooling	Line
WL00011	MRC	3 GB Data Add-on Pooling	Line
WL00012	MRC	5 GB Data Add-on Pooling	Line
WL00013	MRC	10 GB Data Add-on Pooling	Line
WL00020	Usage	Pooling Overage for Data Add-on	GB
WL00030	MRC	Unlimited Data Add-on	Line

B.2.6.3 Domestic Mobile Data Only Service

Domestic Mobile Data Only Service may not be ordered with Domestic Mobile Voice Service. As with Data Add-on Services, the data allocations from all data only plans, except Unlimited Data, are pooled or added together across the agency or customer. A hotspot shall be included at no additional cost with all data only plans.

B.2.6.3.1 Domestic Mobile Data Only Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.6.3.2 Domestic Mobile Data Only Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit
WL00100	MRC	1 GB Data Only Pooling	Line
WL00101	MRC	3 GB Data Only Pooling	Line
WL00102	MRC	5 GB Data Only Pooling	Line
WL00103	MRC	10 GB Data Only Pooling	Line
WL00110	Usage	Pooling Overage for Data Only	GB
WL00120	MRC	Unlimited Data Only (may be limited to a single user per data session)	Line

B.2.6.4 Pricing Catalog Requirements

For Domestic to Non-Domestic Calls and for International Roaming services offered via a catalog, the contractor shall develop and maintain an online catalog of offerings and pricing in accordance with B.1.3.

The MWS catalogs provided by the contractor shall, at a minimum, contain the data elements defined in the tables below. For Domestic to Non-Domestic Calling, this information includes the Country or Jurisdiction ID being called and the termination method (when there is a pricing difference between wireless and wireline termination). For International Mobile Roaming, it includes the Country or Jurisdiction ID from which a communications originated and the relevant number of minutes/texts/MBs. Other information may be provided by the contractor at its option.

Catalog prices for Domestic to Non-Domestic Calls and for International Roaming shall be based on a discount from the Official List Price (OLP). The Class Discount ID determines the discount to be applied to the OLP. The contractor shall identify the trade name(s) for the OLP.

B.2.6.5 Domestic to Non-Domestic Mobile Calling

The Domestic to Non-Domestic Mobile Calling Catalog pricing in Table B.2.6.5.1 shall be based on a discount from the contractor's official supplier's best list price. Discount

classes shall be specified in Table B.2.6.5.2. Charging mechanisms are provided in Table B.2.6.5.3. Catalog items in Table B.2.6.5.1 shall be priced per minute.

B.2.6.5.1 Domestic to Non-Domestic Mobile Calling Catalog Table

CLIN	Case Number	Plan Description	Terminating Country/ Jurisdiction ID*	OLP	OLP Type**	Class Discount ID***	Start Date	Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1
** Use "WIRELESS" if OLP column contains a wireless termination OLP, or "WIRELINE" if OLP column contains a wireline termination OLP
*** From Table B.2.6.5.2

B.2.6.5.2 Domestic to Non-Domestic Mobile Calling Class Discount Table

Class Discount ID*	Class Description	Task Order Number	Percentage Discount from OLP	Start Date	Stop Date
2000					
…					
2999					

* The number of calling classes shall be selected by the contractor from within the range shown

B.2.6.5.3 Domestic to Non-Domestic Mobile Calling Instruction Table

CLIN	Frequency	Description	Charging Unit	Notes
WL01001	Usage	Domestic to Non-Domestic Mobile Calling Catalog Item	Minute	ICB

B.2.6.6 International Mobile Roaming (Optional)

International Mobile Roaming plans (from Non-Domestic to either Domestic or Non-Domestic) shall cover voice calls, messaging, multimedia, and data. They may be purchased independently from any domestic service. There are two types of plans:

1) Data bucket and unlimited plans that cover one or more specified countries
2) Catalog plans

For all plans, the contractor shall provide website links to describe the following:

- The coverage within each country
- Any device requirements to obtain coverage in a country

- Partner Wi-Fi hotspots that are available at no extra cost

For each bucket and unlimited plan excluding the Canada & Mexico plan, the contractor shall list the countries included in the plan and maintain a website link to that list. If usage from a foreign country is included as part of a domestic service plan, then any usage from that country shall be billed against the domestic usage plan, and International Mobile Roaming charges are not applicable.

Both the International Mobile Roaming Bucket and Unlimited Prices Table and the International Mobile Roaming Catalog Table are optional. Therefore, one of the tables may be offered without offering the other table.

B.2.6.6.1 International Mobile Roaming Bucket and Unlimited Prices Table (Optional)

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.6.6.2 International Mobile Roaming Bucket and Unlimited Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
WL01100	MRC	**Canada & Mexico 150 MB Data**: 150 MB of data, unlimited messaging, and unlimited Wi-Fi.	Line	
WL01101	Usage	Data Overage per MB for Canada & Mexico 150 MB Data Plan	MB	
WL01102	Usage	Voice Access for Canada & Mexico 150 MB Data Plan	Minute	
WL01110	MRC	**Global* 300 MB Data**: 300 MB of data, unlimited messaging, and unlimited Wi-Fi.	Line	
WL01111	Usage	Data Overage for Global 300 MB Data Plan	MB	
WL01112	Usage	Voice Access for Global 300 MB Data Plan	Minute	
WL01120	MRC	**Global* 800 MB Data**: 800 MB of data, unlimited messaging, and unlimited Wi-Fi.	Line	Optional

CLIN	Frequency	Description	Charging Unit	Notes
WL01121	Usage	Data Overage for Global 800 MB Data Plan	MB	Optional
WL01122	Usage	Voice Access for Global 800 MB Data Plan	Minute	Optional
WL01130	MRC	**Global* Unlimited Data**: Unlimited non-domestic data, unlimited messaging, and unlimited Wi-Fi on partner networks.	Line	Optional
WL01131	Usage	Voice Access for Unlimited Data Plan	Minute	Optional

* Global coverage shall include, at a minimum, the following countries and territories: Canada, China, France, Germany, Guam, American Samoa, Commonwealth of Northern Marianas Islands, Midway Island, Wake Island, Israel, Japan, Mexico, Netherlands, and United Kingdom.

B.2.6.6.3 International Mobile Roaming Catalog Table (Optional)

CLIN	Case Number	Plan Description	Originating Country / Jurisdiction ID*	OLP	Roaming Class ID**	Start Date	Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

** ID from Table B.2.6.6.4

B.2.6.6.4 International Mobile Roaming Class Discount Table

Roaming Class ID*	Class Description	Task Order Number	Percentage Discount from OLP	Start Date	Stop Date
3000					
…					
3999					

* The number of roaming classes shall be selected by the contractor from within the range shown

B.2.6.6.5 International Mobile Roaming Instruction Table

CLIN	Frequency	Description	Charging Unit	Notes
WL01201	Usage	International Mobile Voice Roaming Catalog Item	Minute	ICB
WL01202	Usage	International Mobile Data Roaming Catalog Item	MB	ICB

CLIN	Frequency	Description	Charging Unit	Notes
WL01203	Usage	International Mobile Roaming Inbound Text Catalog Item	Message	ICB
WL01204	Usage	International Mobile Roaming Outbound Text Catalog Item	Message	ICB

B.2.6.7 Wireless Features

The technical requirements for MWS are defined in Section C.2.6. Wireless features shall be listed in the table below.

B.2.6.7.1 Wireless Feature Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.6.7.2 Wireless Feature Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
WL02000	Usage	Wireless Priority Services (WPS)	Minute	Mandatory where available. No activation or monthly fee shall be charged.
WL02001	Usage	Directory Assistance with Call Completion	Call	Includes being able to retrieve at least two numbers per call and being connected to one of the requested listings.
WL02002	NRC	Domestic to Non-Domestic Calling	Line	NSP. If enabled, usage charges apply. See Section B.2.6.5~~B.2.6.5~~. Allows a user to make non-domestic calls. It shall automatically be included when ordering a voice plan. This feature shall be disabled at agency direction.

Formatte

CLIN	Frequency	Description	Charging Unit	Notes
WL02003	NRC	International Mobile Roaming	Line	NSP. If enabled, usage charges apply. See Section B.2.6.6~~B.2.6.6~~. Allows a user to roam internationally with wireless Internet connectivity and communications capability. It shall automatically be included where available when ordering either a voice or data plan. This feature shall be disabled at agency direction.
WL02004	MRC	Personal Hotspot (5GB minimum) – applicable only to the Unlimited Data Add-on plan.	Line	Personal hotspots are included with all domestic data plans except unlimited data add-on plans.
WL02010	MRC	Push-To-Talk (PTT) with Group Talk	Line	Optional.

Formatte

B.2.6.7.3 Wireless Machine to Machine Pricing (Optional)

MWS pricing for Machine to Machine (M2M) is listed in the table below.

B.2.6.7.3.1 Wireless M2M Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.6.7.3.2 Wireless M2M Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
WL03000	MRC	M2M 1 MB: 1 MB of data per month for M2M devices.	Line	
WL03001	MRC	M2M 2 MB: 2 MB of data per month for M2M devices.	Line	Optional
WL03002	MRC	M2M 5 MB: 5 MB of data per month for M2M devices.	Line	Optional

CLIN	Frequency	Description	Charging Unit	Notes
WL03003	MRC	M2M 25 MB: 25 MB of data per month for M2M devices.	Line	Optional
WL03004	MRC	M2M 50 MB: 50 MB of data per month for M2M devices.	Line	Optional
WL03005	MRC	M2M 250 MB: 250 MB of data per month for M2M devices.	Line	Optional
WL03006	MRC	M2M 1 GB: 1 GB of data per month for M2M devices.	Line	Optional
WL03007	MRC	M2M 5 GB: 5 GB of data per month for M2M devices.	Line	Optional
WL03020	Usage	M2M Overage (<= 50 MB) – Overage for plans up to and including 50 MB of data per month for M2M devices.	MB	
WL03021	Usage	M2M Overage (> 50 MB) – Overage for plans above 50 MB of data per month for M2M devices.	MB	Optional

B.2.6.7.4 Wireless Task Order Unique CLINs

The tables below provide the format and instructions for pricing TUCs supported by Wireless. TUCs shall be used as defined in Section B.1.2.15.

B.2.6.7.4.1 Wireless TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.6.7.4.2 Wireless TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
WL99990	WL99991	WL99992	MWS Task Order Unique	ICB	ICB

B.2.7 Commercial Satellite Communications Service

The technical requirements for Commercial Satellite Communications Service (COMSATCOM) are defined in Section C.2.7. The services include Commercial Mobile Satellite Service (CMSS) and Commercial Fixed Satellite Service (CFSS).

The price structure for COMSATCOM includes the following elements:

1. NRC
2. MRC
3. Usage charges

Features are normally separately priced although some features are defined as NSP. The device equipment required to obtain all services shall be included in the SRE Catalog. Bandwidth throttling (intentional slowing of data speeds by the service provider) is not permitted.

B.2.7.1 Commercial Mobile Satellite Service

Commercial Mobile Satellite Service (CMSS) voice and data pricing is shown in the tables below. Text messages are included under Table B.2.7.1.1.

Data sent using a voice channel (typically at less than 25 Kbps) is charged by the minute. No activation fees shall be charged. All plans shall include voicemail and incoming text messages at no extra cost.

B.2.7.1.1 CMSS Voice Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.7.1.2 CMSS Voice Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
CM00001	MRC	0 Minute Plan	Line	Basic CMSS access with 0 minutes per month included.
CM00002	Usage	0 Minute Plan Usage	Minute	The cost per minute to initiate or receive a phone call.
CM00003	MRC	10 Minute Plan	Line	Optional. CMSS access with 10 minutes per month included.

CLIN	Frequency	Description	Charging Unit	Notes
CM00004	MRC	40 Minute Plan	Line	CMSS access with 40 minutes per month included.
CM00005	MRC	100 Minute Plan	Line	CMSS access with 100 minutes per month included.
CM00006	MRC	300 Minute Plan	Line	Optional. CMSS access with 300 minutes per month included.
CM00020	Usage	Voice Usage Overage – Applicable to all plans but the 0 Minute Plan	Minute	The cost per minute to initiate or receive a phone call beyond the minutes allocated in the voice plan excluding the 0 Minute Plan.
CM00030	MRC	Unlimited Voice Plan	Line	Optional. CMSS access with unlimited number of minutes per month included.
CM00040	Usage	Outgoing Text Message	Message	No charge for inbound text messages.

B.2.7.1.3 CMSS Data

CMSS data pricing is shown in the tables below. Data plans may be defined by the contractor in its catalog as an add-on to a voice plan. Text messages and data sent using a voice channel shall be included in Table B.2.7.1.1. No activation fees shall be charged. The data upload and download speeds and global coverage shall be included in the contractor's proposal. Prepaid and postpaid plans may be offered.

B.2.7.1.4 CMSS Data Pricing Catalog Requirements

The contractor shall develop and maintain an online catalog of offerings and pricing in accordance with Section B.1.3.

The catalog provided by the contractor shall, at a minimum, contain the data elements defined in Table B.2.7.1.5 below. Catalog service descriptions shall specify the amount of data in MBs or GBs that is included in the catalog item. Agency bills shall also reference these catalog data elements, which will be used to calculate the cost.

Catalog prices shall be based on a discount from the OLP. The Data Class ID determines the discount to be applied to the OLP. The contractor shall identify the trade name(s) for the OLP. Catalog prices shall not vary by geographic location.

B.2.7.1.5 CMSS Data Catalog Table

CLIN	Case Number	Service Description	OLP	No List Price*	Data Class ID**	Start Date	Stop Date

* ”T” if the price appearing in the OLP column is not an official supplier list price, “F” otherwise
** From Table B.2.7.1.6

B.2.7.1.6 CMSS Data Class Discount Table

Data Class ID*	Class Description	Task Order Number	Percentage Discount from OLP	Start Date	Stop Date
4000					
…					
4999					

* The number of data classes shall be selected by the contractor from within the range shown

B.2.7.1.7 CMSS Data Instruction Table

CLIN	Frequency	Description	Charging Unit	Notes
CM90002	MRC	CMSS Data Catalog Plan	Line	ICB
CM90003	Usage	CMSS Data Catalog Item	MB	ICB

B.2.7.1.8 CMSS Task Order Unique CLINs

The tables below provide the format and instructions for pricing TUCs supported by CMSS. TUCs shall be used as defined in Section B.1.2.15.

B.2.7.1.9 CMSS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.7.1.10 CMSS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
CM99990	CM99991	CM99992	CMSS Task Order Unique	ICB	ICB

B.2.7.2 Commercial Fixed Satellite Service

The first type of pricing for CFSS is ICB for a fixed level of bandwidth and the applicable installation of the equipment as shown Tables B.2.7.2.1 and B.2.7.2.2 below.

The second type of pricing for CFSS is for Satellite Internet Service as shown in Tables B.2.7.2.3 and B.2.7.2.4 below. The indicated amount of data included in the Satellite Internet Service plan shall be able to be used at any time of the day within domestic regions (as defined in Section B.2.6 of Wireless Service).

B.2.7.2.1 CFSS Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.7.2.2 CFSS Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
FS02000	NRC	CFSS Installation	Terminal	ICB
FS02001	MRC	CFSS Bandwidth	KB	ICB

B.2.7.2.3 Satellite Internet Prices

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.7.2.4 Satellite Internet Pricing Instructions

CLIN	Frequency	Description	Charging Unit	Notes
FS00000	MRC	**15 GB** per month	Line	
FS00002	MRC	**30 GB** per month	Line	
FS00004	MRC	**50 GB** per month	Line	
FS00010	Usage	**Data Overage**	GB	

CLIN	Frequency	Description	Charging Unit	Notes
FS00020	MRC	**Unlimited Domestic Voice** – Includes Call Waiting, Voice Mail, and Caller ID	Line	Optional. A data package may be required to be purchased with this CLIN.
FS00030	MRC	**Unlimited International Voice**	Line	Optional
FS00040	NRC	**Installation** – Includes connectors and cabling to obtain Internet access.	Line	Optional

B.2.7.2.5 CFSS Task Order Unique CLINs

The tables below provide the format and instructions for pricing TUCs supported by CFSS. TUCs shall be used as defined in Section B.1.

B.2.7.2.5.1 CFSS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.7.2.5.2 CFSS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
FS99990	FS99991	FS99992	CFSS Task Order Unique	ICB	ICB

B.2.8 Managed Services

B.2.8.1 Managed Network Service

The technical requirements for Managed Network Service (MNS) are defined in Section C.2.8.1.

The price structure for MNS includes the following elements:

1. NRC
2. MRC
3. Feature Charges

The prices in this section shall cover only the specific technical requirements in Section C.2.8.1. Prices for any associated SRE shall be provided in accordance with Section B.2.10.

B.2.8.1.1 Full Managed Network Service Prices

Full MNS includes the following components:

1. Managed Network Design and Engineering
2. Managed Network Implementation, Management and Maintenance
3. Out-of-Band (OOB) Service

B.2.8.1.2 Managed Network Design and Engineering

Managed Network Design and Engineering shall be priced ICB as an NRC. Table B.2.8.1.2.1 provides the formats for pricing information for Managed Network Design and Engineering. Table B.2.8.1.2.2 provides applicable charging mechanisms and charging units.

B.2.8.1.2.1 Managed Network Design and Engineering Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.8.1.2.2 Managed Network Design and Engineering Pricing Instructions Table

NRC CLIN	Description	Charging Unit	Notes
MN00001	Managed Network Design and Engineering	Device	ICB

B.2.8.1.3 Managed Network Implementation, Management and Maintenance

Table B.2.8.1.3.1 provides the formats for pricing information for Managed Network Implementation, Management and Maintenance. Table B.2.8.1.3.2 provides applicable charging mechanisms and charging units. Table B.2.8.1.3.3 provides optional charging mechanisms and charging units. Prices exclude the cost of bandwidth SRE and SRE maintenance covered by the SRE's MMC. A device under MNS is typically a router, switch, or similar equipment at the user's location that acts as a point of connection between the user's location and the contractor's networking service(s) (e.g., VPNS, Ethernet or Private Line Service).

B.2.8.1.3.1 Managed Network Implementation, Management and Maintenance Prices Table

CLIN*	Case Number**	Task Order Number	Price	Price Start Date	Price Stop Date

* CLINs are listed in Tables B.2.8.1.3.2 and B.2.8.1.3.3
** Applies only to ICB CLINs

B.2.8.1.3.2 Managed Network Implementation, Management and Maintenance Pricing Instructions Table for Managed Devices

NRC CLIN	MRC CLIN	Description	Charging Unit
MN11001	MN10001	Managed Network Implementation, Maintenance and Management, Extra-Small	Device
MN11002	MN10002	Managed Network Implementation, Maintenance and Management, Small	Device
MN11003	MN10003	Managed Network Implementation, Maintenance and Management, Medium	Device
MN11004	MN10004	Managed Network Implementation, Maintenance and Management, Large	Device
MN11005	MN10005	Managed Network Implementation, Maintenance and Management, Extra-Large	Device

B.2.8.1.3.3 Managed Network Implementation, Management and Maintenance Pricing Instructions Table for IP-MPLS Routing

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
MN16001	MN15001	Managed Network Implementation, Maintenance and Management, Base service (IP-MPLS routing)*	Device	Optional
MN16002	MN15002	Router Security Features – add on to Base Service	Device	Optional
MN16003	MN15003	Unified Communications Features – add on to Base Service	Device	Optional

* Routers with basic IP-MPLS services use this base CLIN. Additional features include router-based security features and Unified Communications. A router may have none, one, or both additional features listed above.

B.2.8.1.4 MNS Out-of-Band Service (POTS Line or Wireless Service)

Table B.2.8.1.4.1 provides the format for pricing Out-of-Band (OOB) POTS Line or Wireless Service. Table B.2.8.1.4.2 provides the pricing instructions.

B.2.8.1.4.1 MNS Out-of-Band Access Prices Table

CLIN	Case Number*	Task Order Number	Country / Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.8.1.4.2 MNS Out-of-Band Access Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
MN21002	MN20002	~~CONUS~~ Out-of-Band POTS Line (POTS Line provided by contractor and price includes both line and OOB management)	Device	CONUS and OCONUS only. Device is modem - Modem price and maintenance are SRE
~~MN21004~~	~~MN20004~~	~~OCONUS Out-of-Band POTS Line (POTS Line provided by contractor and price includes both line and OOB management)~~	~~Device~~	~~Device is modem - Modem price and maintenance are SRE~~
MN21021	MN20021	~~CONUS~~ Wireless Out-of-Band Access (Wireless OOB Access provided by contractor and price includes both OOB wireless service and OOB management)	Device	Optional. CONUS and OCONUS only. Device is modem - Modem price and maintenance are SRE
~~MN21023~~	~~MN20023~~	~~OCONUS Wireless Out-of-Band Access (Wireless OOB Access provided by contractor and price includes both OOB wireless service and OOB management)~~	~~Device~~	~~Optional. Device is modem - Modem price and maintenance are SRE~~

B.2.8.1.5 MNS Features

Table B.2.8.1.5.1 provides the formats for pricing information for MNS features. Table B.2.8.1.5.2 provides applicable charging mechanisms and charging units for MNS features.

B.2.8.1.5.1 MNS Feature Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.8.1.5.2 MNS Feature Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
MN51001	MN50001	Government Furnished Property Maintenance	Device	ICB
MN31001	MN30001	Agency-Specific Network Operations Center (NOC)	Proposal	ICB
MN34001	MN33001	Agency-Specific Security Operations Center (SOC)	Proposal	ICB
MN52002	MN52001	Traffic Aggregation Service (DHS)*	ICB	ICB. DHS only

*The traffic aggregation service may only be ordered by DHS, and costs must be separate and distinct from agency transport costs. Agencies maintain all responsibility for their transport costs. All charges for traffic aggregation service are to be incurred by DHS and none by the agencies.

B.2.8.1.6 MNS Task Order Unique CLINs

Table B.2.8.1.6.1 provides the format for pricing TUCs supported by MNS. Table B.2.8.1.6.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.8.1.6.1 MNS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.1.6.2 MNS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
MN99990	MN99991	MN99992	MNS Task Order Unique	ICB	ICB

B.2.8.2 Web Conferencing Service

The technical requirements for the Web Conferencing Service (WCS) are defined in Section C.2.8.2.

B.2.8.2.1 Web Conferencing Price Structure

WCS has two pricing options that depend upon the model selected: 1) Subscription Model or 2) Usage Model.

The price structure for WCS includes the following elements:

1. MRC for the Subscription Model
2. Usage charges for the Usage Model
3. Event-based charges
4. Feature charges

WCS may use underlying transport services that may be IP centric (such as VPNS or IPS). Voice or toll-free service may also be used to provide connectivity. These transport services are charged separately.

SRE pricing for the user-to-network interfaces shall be provided in accordance with Section B.2.10.

B.2.8.2.2 Web Conferencing Basic Service

This section provides pricing instructions for the subscription model.

The subscription model is priced on a monthly basis, and offers unlimited web conferences for a maximum number of concurrent participants as specified by the contractor. The maximum number of active hosts may be unlimited depending upon licensing arrangements.

Table B.2.8.2.2.1 provides pricing information for the WCS subscription model. Table B.2.8.2.2.2 provides applicable charging mechanisms and charging units.

B.2.8.2.2.1 Web Conferencing Subscription-Based Prices Table

CLIN	Task Order Number	Band Low*	Band High*	Variable Price	Price Start Date	Price Stop Date

* Price bands reflect the number of enterprise subscribers. Contractor may propose pricing for multiple bands using the same CLIN.

B.2.8.2.2.2 Web Conferencing Subscription-Based Pricing Instructions Table

MRC CLIN	Description	Charging Unit
WC00001	Enterprise license	Enterprise Subscriber

B.2.8.2.3 Web Conferencing Usage-Based Service

Table B.2.8.2.3.1 provides pricing information for WCS usage-based services. Table B.2.8.2.3.2 provides applicable charging mechanisms and charging units.

B.2.8.2.3.1 Web Conferencing Usage Based Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.2.3.2 Web Conferencing Usage-Based Pricing Instructions Table

Usage CLIN	Description	Charging Unit
WC00010	WCS Usage	Minute per participant*

* Usage minutes shall be multiplied by the number of participants to obtain the quantity for charging purposes

B.2.8.2.4 Web Conferencing Service Reservation-Based Events

Table B.2.8.2.4.1 provides pricing information for WCS event-based services. Table B.2.8.2.4.2 provides applicable charging mechanisms and charging units. An event involving either audio or video streaming may be ordered using the applicable CLIN from Table B.2.8.2.4.2 in multiples of 15-minute increments.

B.2.8.2.4.1 Web Conferencing Event-Based Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.2.4.2 Web Conferencing Event-Based Pricing Instructions Table

Usage CLIN	Description	Charging Unit
WC00100	Audio Streaming (includes visuals) for up to 1000 attendees, 15 minute increment	15 minutes
WC00102	Audio Streaming (includes visuals) for 1001-2000 attendees, 15 minute increment	15 minutes
WC00104	Audio Streaming (includes visuals) for 2001-3000 attendees, 15 minute increment	15 minutes
WC00110	Video Streaming (includes visuals) for up to 1000 attendees, 15 minute increment	15 minutes
WC00112	Video Streaming (includes visuals) for 1001-2000 attendees, 15 minute increment	15 minutes
WC00114	Video Streaming (includes visuals) for 2001-3000 attendees, 15 minute increment	15 minutes

B.2.8.2.5 Web Conferencing Features

Table B.2.8.2.5.1 provides pricing instructions for the features supported by WCS. Table B.2.8.2.5.2 provides applicable charging mechanisms and charging units.

B.2.8.2.5.1 Web Conferencing Feature Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.2.5.2 Web Conferencing Feature Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
WC90001	MRC	Web Based Presentation Additional Storage for Replay	GB	Price for initial 90 days included with basic service. The maximum number of increments is 9; one for each month for a total period of 12 months.
WC90002	Usage	Web Based Presentation Replay	Each	NSP

B.2.8.2.6 Web Conferencing Task Order Unique CLINs

Table B.2.8.2.6.1 provides the format for pricing TUCs supported by WCS. Table B.2.8.2.6.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.8.2.6.1 Web Conferencing TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.2.6.2 Web Conferencing TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
WC99990	WC99991	WC99992	WCS Task Order Unique	ICB	ICB

B.2.8.3 Unified Communications Service

Unified Communication Service (UCS) is an application hosted by the contractor that provides unified communications to multiple users using an agency-provided (managed), contractor-provided (hosted), or hybrid solution. The technical requirements for UCS are defined in Section C.2.8.3.

The price structure for UCS includes the following elements:

1. Design and Engineering
2. Service

B.2.8.3.1 Unified Communications Design and Engineering Price Structure

Achieving a seamless UCS implementation requires an evaluation of the agency's current voice, data and applications environments. The CLIN associated with the UCS

Design and Engineering service shall be priced ICB. SRE pricing for required equipment (e.g., user interface devices) shall be provided in accordance with Section B.2.10.

B.2.8.3.1.1 Unified Communications Design and Engineering Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.8.3.1.2 Unified Communications Design and Engineering Pricing Instructions Table

NRC CLIN	Description	Charging Unit	Notes
UC11001	Network Design and Engineering Service	Solution	ICB

B.2.8.3.2 Unified Communications Service Price Structure

B.2.8.3.2.1 Unified Communications CONUS Service Prices Table

CLIN	Case Number*	Task Order Number	Band Low**	Band High**	Variable Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Price bands reflect the number of seats. Contractor may propose pricing for multiple bands using the same CLIN.

B.2.8.3.2.2 Unified Communications OCONUS and Non-Domestic Service Prices Table

CLIN	Case Number*	Task Order Number	Country/ Jurisdiction ID**	Band Low***	Band High***	Variable Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1
*** Price bands reflect the number of seats. Contractor may propose pricing for multiple bands using the same CLIN.

B.2.8.3.2.3 Unified Communications Service Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
UC21001	UC22001	Hosted UCS Unlimited*	Seat	
UC31001	UC32001	Managed UCS Unlimited*	Seat	ICB
UC51001	UC52001	Hybrid UCS Unlimited*	Seat	ICB

* Unlimited Calls/Fax/SMS/Conferencing

B.2.8.3.3 Unified Communications Task Order Unique CLINs

Table B.2.8.3.3.1 provides the format for pricing TUCs associated with UCS. Table B.2.8.3.3.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.8.3.3.1 Unified Communications TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.3.3.2 Unified Communications TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
UC99990	UC99991	UC99992	UCS Task Order Unique	ICB	ICB

B.2.8.4 Managed Trusted Internet Protocol Service

The technical requirements for Managed Trusted Internet Protocol Service (MTIPS) are defined in Section C.2.8.4.

B.2.8.4.1 MTIPS Price Structure

The price structure for MTIPS includes the following elements:

1. MRC
2. Feature Charges

MTIPS Trusted Internet Connection (TIC) SOC equipment for mandatory security functions shall be included in the MTIPS basic service price. Pricing for MTIPS-

associated SRE, such as routers at the agency location, shall be listed in the SRE Catalog. If the contractor provides any optional MTIPS security functions, then the contractor shall price those security functions using the corresponding Managed Security Service prices (Section B.2.8.5).

B.2.8.4.2 MTIPS Access

The contractor shall allow agencies to connect to the contractor's MTIPS transport network using access arrangements as described in Section B.2.9.

B.2.8.4.3 MTIPS Basic Service

The contractor shall price MTIPS with an MRC CLIN based on port bandwidth. The MTIPS port price shall include the TIC Portal Capabilities, the Transport Collection and Distribution Capabilities, the Network Operations and Management, and TIC Portal SOC FISMA A&A, as specified in Section C.2.8.4.

B.2.8.4.4 MTIPS Price Structure

Table B.2.8.4.4.1 provides the format for MTIPS port prices. Table B.2.8.4.4.2 provides the instructions for pricing MTIPS in domestic and non-domestic country/jurisdictions. The contractor shall price the optional MTIPS E1 and E3 ports in non-domestic country/jurisdictions only.

B.2.8.4.4.1 MTIPS Port Prices Table

CLIN	Case Number*	Task Order Number	Country / Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.8.4.4.2 MTIPS Port Pricing Instructions Table

MRC CLIN	Description	Charging Unit	Notes
MT00001	MTIPS - T1	Port	Optional
MT00002	MTIPS - FT3 - 3 Mbps	Port	Optional
MT00003	MTIPS - FT3 - 6 Mbps	Port	Optional
MT00004	MTIPS - FT3 - 10 Mbps	Port	Optional
MT00005	MTIPS - T3	Port	
MT00006	MTIPS - OC3c (155 Mbps)	Port	

MRC CLIN	Description	Charging Unit	Notes
MT00008	MTIPS - OC12c (622 Mbps)	Port	
MT00010	MTIPS - OC48c (2.5 Gbps)	Port	Optional
MT00012	MTIPS - OC192c (10 Gbps)	Port	Optional
MT00031	MTIPS - Ethernet – 10 Mbps	Port	Optional
MT00032	MTIPS - Ethernet – 20 Mbps	Port	Optional
MT00033	MTIPS - Ethernet – 30 Mbps	Port	Optional
MT00034	MTIPS - Ethernet – 40 Mbps	Port	Optional
MT00035	MTIPS - Ethernet – 50 Mbps	Port	Optional
MT00041	MTIPS - Ethernet – 100 Mbps	Port	Optional
MT00042	MTIPS - Ethernet – 200 Mbps	Port	
MT00043	MTIPS - Ethernet – 300 Mbps	Port	Optional
MT00044	MTIPS - Ethernet – 400 Mbps	Port	Optional
MT00045	MTIPS - Ethernet – 500 Mbps	Port	
MT00051	MTIPS - Ethernet – 1 Gbps	Port	
MT00060	MTIPS - Ethernet – 10 Gbps	Port	
MT00061	MTIPS - E1	Port	Optional. Non-domestic only
MT00062	MTIPS - E3	Port	Optional. Non-domestic only

SRE pricing for the user-to-network interfaces shall be provided in accordance with Section B.2.10.

B.2.8.4.5 MTIPS Feature Prices

Table B.2.8.4.5.1 provides the format for MTIPS feature prices. Table B.2.8.4.5.2 provides the pricing instructions for pricing the domestic MTIPS features.

B.2.8.4.5.1 MTIPS Feature Prices Table

CLIN	Case Number*	Task Order Number	Country/ Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.8.4.5.2 MTIPS Feature Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
MT90011	MRC	Encrypted Traffic	ICB	ICB
MT90012	MRC	Agency Security Policy Enforcement	ICB	ICB
MT90013	MRC	Forensic Analysis	ICB	ICB
MT90014	MRC	Custom Reports	Report	ICB
MT91001	NRC	Agency NOC/SOC Console	ICB	ICB
MT91002	MRC	Agency NOC/SOC Console	ICB	ICB
MT91003	MRC	Custom Security Assessment and Authorization Support (previously known as “Custom Certification and Accreditation (C&A) Support”)	Proposal	ICB
MT91004	NRC	Custom Security Assessment and Authorization Support (previously known as “Custom Certification and Accreditation (C&A) Support”)	Proposal	ICB
MT91005	MRC	External Network Connection	Connection	ICB
MT91006	NRC	External Network Connection	Connection	ICB
MT91013	MRC	Encrypted DMZ	ICB	ICB
MT91014	MRC	Encrypted DMZ - One security device	Each	
MT91015	MRC	Remote Access (CONUS and OCONUS, 1 seat)	Seat	
MT91016	MRC	Remote Access (CONUS and OCONUS, 2 - 5 seats)	Seat	
MT91017	MRC	Remote Access (CONUS and OCONUS, 6 – 50 seats)	Seat	
MT91018	MRC	Remote Access (CONUS and OCONUS, 51 – 100 seats)	Seat	
MT91019	MRC	Remote Access (CONUS and OCONUS, 101+ seats)	Seat	ICB
MT91020	MRC	Custom Remote Access	Seat	ICB
MT91021	MRC	Extranet Connection (CONUS and OCONUS, 1 user at the node)	Node	
MT91022	MRC	Extranet Connection (CONUS and OCONUS, 2-to-5 users at the node)	Node	
MT91023	MRC	Extranet Connection (CONUS and OCONUS, 6-to-50 users at the node)	Node	

CLIN	Frequency	Description	Charging Unit	Notes
MT91024	MRC	Extranet Connection (CONUS and OCONUS, 51-to-100 users at the node)	Node	
MT91025	MRC	Extranet Connection (CONUS and OCONUS,100+ users at the node)	Node	ICB
MT91026	MRC	Custom Extranet Connection	Node	ICB
MT91027	MRC	Inventory Mapping Service	Network	ICB

B.2.8.4.6 MTIPS Task Order Unique CLINs

Table B.2.8.4.6.1 provides the format for pricing the TUCs supported by MTIPS. Table B.2.8.4.6.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.8.4.6.1 MTIPS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.4.6.2 MTIPS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
MT99990	MT99991	MT99992	MTIPS Task Order Unique	ICB	ICB

B.2.8.5 Managed Security Service

The technical requirements for Managed Security Service (MSS) are defined in Section C.2.8.5. MSS mandatory services are:

1. Managed Prevention Service
2. Vulnerability Scanning Service
3. Incident Response Service

Many providers offer an array of potential services and service variations, as well as special tailored services, which use or span the MSS mandatory services. For pricing purposes, the contractor shall provide an MSS Catalog consistent with the service requirements in Section C.2.8.5, and with the pricing catalog requirements in Section

B.1.3. The contractor shall use Managed Security Service Category Reference Table B.2.8.5.4 to relate its offerings to the MSS mandatory services.

B.2.8.5.1 Catalog Requirements for Pricing Information

Where MSS offerings include equipment, all MSS-related equipment or equipment features shall be identified and priced in accordance with the SRE requirements in Section B.2.10. Where MSS-related labor is offered, then labor rates shall be specified and priced in accordance with Section B.2.11.

Otherwise, MSS prices for non-labor and non-SRE elements shall be determined from the catalog based on the information required as shown in Table B.2.8.5.2 below. Charging mechanisms are defined in Table B.2.8.5.5. Additional discounts or reduced prices may be negotiated at time of TO award between the ordering agency and the contractor.

B.2.8.5.2 Managed Security Service Catalog – Product Specification Table

CLIN	Case Number	Category *	Service Description**	OLP	No List Price***	Service Class ID	Start Date	Stop Date	End of Sale Date****	End of Life Date*****	Notes
		(from Table B.2.8.5.4)				*(from Table B.2.8.5.3~~B.2.8.5.3~~)*					

Formatte

* An array value containing all category codes from Table B.2.8.5.4 corresponding to the services provided by the catalog item.
** Descriptions shall be sufficiently complete that all capabilities and limitations of the MSS, as priced, are clear to the government
*** "T" if the price appearing in the OLP column is not an official list price, "F" otherwise
**** End of Sale Date shall be the effective date after which an item may no longer be purchased. Stop Date shall not be later than End of Sale Date.
***** End of Life Date shall be the effective date after which an item is no longer supported by the contractor

The discount to be applied to the OLP is determined by the Service Class, as shown in Table B.2.8.5.3. The contractor shall identify the trade name(s) for the OLP. The MSS NRC, MRC and/or Usage price shall be the OLP, less the discount for the service class. If no OLP exists, the contractor shall specify its price in the OLP column, populate the No List Price column with "T", and assign a Service Class ID where the discount is 0% (i.e., Service Class 5000).

B.2.8.5.3 Managed Security Service Catalog – Service Class Discount Table

Service Class ID*	Service Class Description**	Task Order Number	Percentage Discount from OLP	Start Date	Stop Date
5000	(e.g., No discount)		0		
5001					
…					
5999					

* The number of service classes shall be selected by the contractor from within the range shown
** The service class description and percentage discount for each service class shall be fixed through the life of the contract, unless changed by contract modification. The Start and Stop Dates shall only apply when a change is caused by contract modification.

The Service Class discount and catalog price shall not vary by geographic location.

The contractor shall assign each item in MSS Catalog Table B.2.8.5.2 to one or more of the MSS categories listed in Reference Table B.2.8.5.4. Additional MSS categories may be defined upon request by the contractor.

B.2.8.5.4 Managed Security Service Category Reference Table

Category	Category Description
1	Managed Prevention Service (MPS)
2	Vulnerability Scanning Service (VSS)
3	Incident Response Service (INRS)

B.2.8.5.5 Managed Security Service Instruction Table

CLIN	Frequency	Description	Charging Unit	Notes
MS90001	NRC	Managed Security Service Catalog Item	ICB	ICB
MS90002	MRC	Managed Security Service Catalog Item	ICB	ICB
MS90003	Usage	Managed Security Service Catalog Item	ICB	ICB

B.2.8.6 Managed Mobility Service

The technical requirements for Managed Mobility Service (MMS) are defined in Section C.2.8.6.

The price structure for MMS includes the following elements:

1. NRC
2. MRC
3. Usage charges

All MRC prices are per device unless specified otherwise. Features are normally separately priced although some features have been defined as NSP. All NSP items shall have a price of zero ($0) entered in the price tables.

Software upgrades shall be included in the price of all MRC subscription software.

B.2.8.6.1 Mobile Device Management

Mobile Device Management (MDM) enables agencies to manage and secure data on a device, including providing enterprise email access. All MDM services listed in the tables below shall meet the security requirements in Section C.2.8.6.1.4.3.

The contractor shall provide at least one of the license alternatives in Table B.2.8.6.1.2.

B.2.8.6.1.1 MDM Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.6.1.2 MDM Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
MM00001	MRC	On Premises MDM License Per Device	Device	License
MM00002	MRC	On Premises MDM License Per User with up to three devices per user	User	License
MM00030	MRC	Cloud MDM License Per Device	Device	License
MM00031	MRC	Cloud MDM License Per User with up to three devices per user	User	License

B.2.8.6.2 Mobile Application Management

Mobile Application Management (MAM) manages device applications. MAM includes the following capabilities (see Section C.2.8.6.1.4.2):

1) Application deployment
2) Mobile Application Store (MAS)
3) Application security

The contractor shall provide at least one of the license alternatives in Table B.2.8.6.2.2.

B.2.8.6.2.1 MAM Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.6.2.2 MAM Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
MM01000	MRC	On Premises MAM License Per Device	Device	License
MM01001	MRC	On Premises MAM License Per User with up to three devices per user	User	License
MM01030	MRC	Cloud MAM License Per Device	Device	License
MM01031	MRC	Cloud MAM License Per User with up to three devices per user	User	License

B.2.8.6.3 Mobile Content Management

Mobile Content Management (MCM) includes securely managing files for a single user across devices or between users for file sharing.

The contractor shall provide at least one of the license alternatives in Table B.2.8.6.3.2.

B.2.8.6.3.1 Content Management Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.6.3.2 Content Management Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
MM02010	MRC	On Premises File Sharing Per User with unlimited data storage scalability	User	License
MM02000	MRC	Cloud File Sharing Per User with unlimited storage (minimum of 1 TB of online storage per user)	User	License

B.2.8.6.4 MMS Task Order Unique CLINS

The tables below provide the format and instructions for pricing TUCs supported by MMS. TUCs shall be used as defined in Section B.1.2.15.

B.2.8.6.4.1 MMS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.6.4.2 MMS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
MM99990	MM99991	MM99992	MMS Task Order Unique	ICB	ICB

B.2.8.7 Audio Conferencing Service

The technical requirements for Audio Conferencing Service (ACS) are defined in Section C.2.8.7.

B.2.8.7.1 ACS Price Structure

The price structure for ACS shall comprise the following elements:

1. NRC for Reservation Charges
2. Usage Charges per bridge for basic ACS
3. Usage Charges for attendant assisted ACS
4. Feature Charges

ACS may use underlying transport services such as landline voice service (CSVS, IPVS) or cellular voice service to provide connectivity. Charges for underlying transport services and dial-in costs are in addition to the charges specified in this section.

B.2.8.7.2 ACS Basic Service Prices

Table B.2.8.7.2.1 provides basic usage pricing for ACS. Table B.2.8.7.2.2 provides pricing instructions for the basic ACS usage prices.

B.2.8.7.2.1 ACS Basic Usage Prices Table

CLIN	Task Order Number	Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.8.7.2.2 ACS Basic Usage Pricing Instructions Table

Usage CLIN	Description	Charging Unit	Notes
AC11001	Audio Conferencing Service	Bridge port per minute	
AC11002	Domestic toll free dial-in Transport	Bridge port per minute	Optional
AC11003	Canada toll free dial-in Transport	Bridge port per minute	Optional
AC11004	Operator dial-out port	Bridge port per minute	
AC11005	Host dial-out port	Bridge port per minute	
AC11006	Executive bridge port	Bridge port per minute	
AC11007	Executive operator dial-out port	Bridge port per minute	
AC11008	Operator Dial-Out Transport	Bridge port per minute	Optional
AC11009	Host Dial-Out Transport	Bridge port per minute	Optional
AC11012	International Global Meet	Bridge port per minute	OCONUS and Non-Domestic only
AC11013	Host Controls	Bridge port per minute	

B.2.8.7.3 ACS Reservation Prices

Table B.2.8.7.3.1 provides the pricing format for ACS reservation service. Table B.2.8.7.3.2 provides pricing instructions.

Reservation charges shall be non-refundable in the event of cancellation of a scheduled conference less than 30 minutes before a conference is scheduled to occur.

B.2.8.7.3.1 ACS Reservation Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.7.3.2 ACS Reservation Pricing Instructions Table

Usage CLIN	Description	Charging Unit
AC21001	ACS Reservation Service	Conference
AC21002	Executive unused reserved port	Bridge port per minute
AC21003	Reservation-less Automated Dial In (RADI) - Toll Free	Bridge port per minute
AC21004	Reservation-less Automated Dial In (RADI) - Caller Paid	Bridge port per minute
AC21005	Reserved Automated Dial In (ADI) - Toll Free	Bridge port per minute
AC21006	Reserved Automated Dial In (ADI) - Caller Paid	Bridge port per minute
AC21009	Reservation Audio Files	Conference

B.2.8.7.4 ACS Attendant Assisted Prices

Table B.2.8.7.4.1 provides pricing format for attendant-assisted ACS. Table B.2.8.7.4.2 provides pricing instructions.

B.2.8.7.4.1 ACS Attendant Assisted Prices Table

CLIN	Task Order Number	Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.8.7.4.2 ACS Attendant Assisted Pricing Instructions Table

Usage CLIN	Description	Charging Unit
AC31001	Attendant-Assisted ACS	15 minutes

B.2.8.7.5 ACS Feature prices

Table B.2.8.7.5.1 provides the format for pricing information for ACS features. Table B.2.8.7.5.2 provides the feature pricing instructions.

B.2.8.7.5.1 ACS Feature Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.8.7.5.2 ACS Feature Pricing Instructions Table

Usage CLIN	Description	Charging Unit	Notes
AC41002	Audio Recording of Call – Removable Storage Media	Each	
AC41005	Language translation – all languages other than Spanish	Translation	ICB, Optional
AC41006	Language translation – Spanish	Translation	
AC41007	Moderator led questions and answers	15 minutes	
AC41008	Participant list report	Report	
AC41009	Password screening	Screening	
AC41010	Replay of pre-recorded audio conference	Replay	
AC41011	Transcription of pre-recorded audio call	Transcription	
AC41012	Temporary blocking of ports	Conference call	
AC41013	Secured Audio Conference	Conference call	Optional

B.2.8.7.6 ACS Task Order Unique CLINs

Table B.2.8.7.6.1 provides the format for pricing TUCs associated with ACS. Table B.2.8.7.6.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.8.7.6.1 ACS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.7.6.2 ACS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
AC99990	AC99991	AC99992	ACS Task Order Unique	ICB	ICB

B.2.8.8 Video Teleconferencing Service

The technical requirements for Video Teleconferencing Service (VTS) are defined in Section C.2.8.8.

B.2.8.8.1 VTS Price Structure

The price structure for VTS includes the following elements:

1. NRC
2. MRC per port for dedicated VTS ports
3. Usage Charges per minute per port for dial-in or dial-out VTS ports
4. Feature Charges

VTS may use underlying transport services to provide connectivity, such as CSDS or PLS. Charges for underlying transport services are in addition to charges specified in this section.

B.2.8.8.2 VTS Basic Service Prices

Table B.2.8.8.2.1 provides pricing for VTS service. Table B.2.8.8.2.2 provides pricing instructions.

Prices for dedicated and dial-in VTS shall be in addition to any applicable charges for the underlying access and transport service used for video teleconferencing. The prices for dial-out VTS shall include the transport and terminating access charges to the user. The Country/Jurisdiction ID shall represent the terminating location when dialing out and the originating location when dialing in.

B.2.8.8.2.1 VTS Prices Table

CLIN	Task Order Number	Country/ Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

Conferences canceled prior to scheduled start time shall not be billable. After the scheduled start time, all reserved ports and features shall be billed for the entire reserved duration whether actually used or not. An ongoing conference that is interrupted through no fault of any of the active participating locations shall be billed at the next lower completed billing increment, and if such an ongoing conference is interrupted in the first billable time increment, there shall be no billing for any time of that conference session.

B.2.8.8.2.2 VTS Service Pricing Instructions Table

Usage CLIN	Description	Charging Unit	Notes
VC11001	Dial-in audio-only capability	Minute per port	
VC11002	Dial-in 384 Kbps or lower (but higher than 128 Kbps) video bandwidth originating at ISDN site	Minute per port	
VC11003	Dial-in 384 Kbps or lower (but higher than 128 Kbps) video bandwidth originating at IP site	Minute per port	
VC11004	Dial-in 768 Kbps or lower (but higher than 384 Kbps) video bandwidth originating at IP site	Minute per port	
VC11005	Dial-out 384 Kbps or lower (but higher than 128 Kbps) video bandwidth terminating at ISDN site	Minute per port	
VC11006	Dial-out 384 Kbps or lower (but higher than 128 Kbps) video bandwidth terminating at IP site	Minute per port	
VC11007	Dial-in 1.92 Mbps or lower (but higher than 768 Kbps) video bandwidth originating at IP site	Minute per port	Optional
VC11010	IEEE 802.3 (IPV4 and IPV6) Ethernet interface up to 10 Mbps	Minute per port	
VC11011	IEEE 802.3 (IPV4 and IPV6) Ethernet interface up to 100 Mbps	Minute per port	

B.2.8.8.3 VTS Feature prices

Table B.2.8.8.3.1 provides the format for pricing information for VTS features. Table B.2.8.8.3.2 provides the feature pricing instructions.

B.2.8.8.3.1 VTS Feature Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.8.3.2 VTS Feature Pricing Instructions Table

CLIN	Frequency	Description	Charging Unit	Notes
VC21001	Usage	Attended Service	Minute	
VC21002	NRC	Verification	Site	
VC21003	Usage	Coding Conversion (Transcoding) Compliant with FTR 1080 Formats	Minute per port	
VC21004	NRC	Rate Adaptation	Conference	Optional
VC21006	Usage	Security – CUI	Minute	Optional

B.2.8.8.4 VTS Task Order Unique CLINs

Table B.2.8.8.4.1 provides the format for pricing TUCs associated with VTS. Table B.2.8.8.4.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.8.8.4.1 VTS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.8.4.2 VTS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
VC99990	VC99991	VC99992	VTS Task Order Unique	ICB	ICB

B.2.8.9 DHS Intrusion Prevention Security Service

The technical requirements for DHS Intrusion Prevention Security Service (IPSS) are defined in Section C.2.8.9.

The price structure for IPSS includes the following elements:

1. NRC
2. MRC
3. Feature Charges

The prices in this section shall cover only the specific technical requirements in Section C.2.8.9. Prices for any associated SRE shall be provided in accordance with Section B.2.10.

B.2.8.9.1 DHS Intrusion Prevention Security Service Price Structure

The CLIN associated with IPSS shall be priced ICB. SRE pricing for required equipment shall be provided in accordance with Section B.2.10. Table B.2.8.9.1.1 provides the formats for pricing information for IPSS. Instruction Table B.2.8.9.1.2 provides the pricing information and charging units.

B.2.8.9.1.1 IPSS Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.8.9.1.2 IPSS Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
DI00001	DI10002	Intrusion Prevention Security Service	ICB	ICB. DHS only

B.2.8.9.2 DHS Intrusion Prevention Security Service Feature Price Structure

Table B.2.8.9.2.1 provides the format for pricing the features supported by IPSS. Instruction table B.2.8.9.2.2 provides the pricing information and charging units.

B.2.8.9.2.1 IPSS Feature Prices Table

CLIN	Case Number*	Task Order Number	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs

B.2.8.9.2.2 IPSS Feature Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
DI11001	DI12001	DHS Email Threat Detection and Countermeasures	ICB	ICB. DHS only
DI11003	DI12003	DHS DNS Threat Detection and Countermeasures	ICB	ICB. DHS only

B.2.8.9.3 DHS Intrusion Prevention Security Service Task Order Unique CLINs

Table B.2.8.9.3.1 provides the format for pricing TUCs supported by IPSS. Table B.2.8.9.3.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.8.9.3.1 IPSS TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.8.9.3.2 IPSS TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
DI99990	DI99991	IPSS Task Order Unique	ICB	ICB. DHS only

B.2.9 Access Arrangements

B.2.9.1 Access Arrangements Pricing

The technical requirements for Access Arrangements (AAs) are defined in Section C.2.9.

AAs connect the customer location to the contractor's POP. When the customer location is at the contractor's POP, no access charges shall apply. For pricing purposes, access is categorized in two ways:

1. Access Arrangements, which are priced within this section, connect the customer location to the contractor's network POP
2. Embedded access, where access prices are included with other service-specific prices, is defined in Section B.2

Switched access (both originating and terminating access) for CSDS, CSVS and TFS is always embedded, and its price is included in the applicable telecommunications service price. Switched access to other services may also be embedded. Access-related pricing information is found in the pricing section for the service being accessed.

SRE is not part of AA, but SRE is often used to meet the service requirements at the SDP when implemented between an access arrangement and the SDP(s). Prices for SRE required for use with AA to provide end-to-end service shall be provided in accordance with Section B.2.10.

For requirements regarding fixed pricing for non-domestic access, see Section J.1.3.2.

AA shall only be used in conjunction with other services provided under this contract. The price for providing access includes one or more of the following elements:

1. NRC
2. MRC
3. Usage
4. Feature Charges

For pricing purposes, the physical address of the SDP location will determine the PHub and will be used for the provision of access. See Section B.4.1 for PHub definitions and requirements.

Domestic Access MRCs depend on the specific access type used to provide the connection defined by the CLIN and a PHub. A PHub is used to group all locations with the same price and the same access service type to a unique identifier. PHubs are used only for pricing purposes. The contractor may decide to arrange pricing so that the PHubs reflect the physical concentration locations (PCLs). The contractor selects and assigns a PHub by Building NSC and access type. Five access types are defined for EIS:

1. Wireline Access
2. Ethernet Access
3. Cable Access
4. Fiber to the Premises (FTTP)
5. Wireless Access

PHubs do not apply to Non-Domestic MRCs. Access NRCs shall not vary by PHub, but may vary by country/jurisdiction.

Access prices for a location shall not increase as a result of NSC/PCL/PHub additions, deletions, redefinitions or relationship changes.

Tables B.2.9.1.1, **Error! Reference source not found.**~~B.2.9.1.1.1~~, B.2.9.1.1.1~~B.2.9.1.2~~, B.2.9.1.3 and B.2.9.1.4 provide the formats for pricing information for access. Table **Error! Reference source not found.**~~B.2.9.1.1.1~~ shall be used to price domestic MRC and Usage ICB CLINs from Table B.2.9.1.5. Table B.2.9.1.5 provides applicable charging mechanisms and charging units and includes a charging mechanism for Scalable Ethernet Access.

Scalable Ethernet Access is ordered in anticipation of a future, temporary need for increased capacity. Scalable Shared Ethernet Access CLINs shall guarantee a committed bandwidth while ensuring the availability of the increased capacity. An Ethernet Access Bandwidth-on-Demand usage CLIN shall provide the increased capacity and must be ordered for the period of time during which the increased capacity will be required. An example of a valid CLIN pairing is Ethernet Access Bandwidth-on-Demand usage CLIN AA00920 used with scalable Shared Ethernet Access MRC CLIN AA00901.

Table B.2.9.1.5 includes an expedited provisioning CLIN that shall be used to provision, within 24 hours rather than the standard provisioning period, an Ethernet Access CLIN at a higher bandwidth, provided the new access CLIN does not exceed the physical capacity of the existing access. This 24-hour provisioning shall be accomplished by ordering the expedited provisioning CLIN concurrent with the new, higher bandwidth Ethernet Access CLIN.

B.2.9.1.1 Domestic Access Prices Table (MRC and Usage)

CLIN	Case Number*	Task Order Number	PHub ID**	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Pricing Hubs (as defined in B.4.1.7)

B.2.9.1.1.1 Domestic Access ICB Prices Table (MRC and Usage)

CLIN	Case Number	Task Order Number	NSC	Price	Price Start Date	Price Stop Date

B.2.9.1.2 Non-Domestic Access Prices Table (MRC and Usage)

CLIN	Case Number*	Task Order Number	NSC	Country/ Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.9.1.3 Domestic Access Prices Table (NRC)

NRC CLIN	Case Number*	Task Order Number	Country/ Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.9.1.4 Non-Domestic Access Prices Table (NRC)

NRC CLIN	Case Number*	Task Order Number	NSC	Country/ Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.9.1.5 Access Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
Wireline Access					
AA00001	AA00101		Basic Subscriber Line (4 KHz)	Circuit	Mandatory if PLS analog transport or CSVS is offered, optional otherwise

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
AA00002	AA00102		DS0	Circuit	
AA00003	AA00103		T1 (1.536 Mbps)	Circuit	
AA00004	AA00104		ISDN PRI	Circuit	
AA00005	AA00105		ISDN BRI	Circuit	
AA00006	AA00106		T3 (43.008 Mbps)	Circuit	
AA00007	AA00107		OC-3c	Circuit	
AA00008	AA00108		OC-12c	Circuit	ICB
AA00009	AA00109		OC-48c	Circuit	ICB
AA00010	AA00110		OC-192c	Circuit	ICB
AA00011	AA00111		OC-768c	Circuit	ICB, Optional
AA00012	AA00112		E1	Circuit	
AA00013	AA00113		E3	Circuit	
AA00014	AA00114		OWS 1 Gbps	Circuit	ICB
AA00015	AA00115		OWS 2.5 Gbps / OC-48	Circuit	ICB
AA00016	AA00116		OWS 10 Gbps/OC-192	Circuit	ICB
AA00017	AA00117		OWS 40 Gbps/OC-768	Circuit	ICB, Optional
AA00018	AA00118		DFS Fiber Pair	Fiber pair	ICB, Optional
AA00019	AA00119		SDSL – up to 1.5 Mbps	Circuit	ICB
AA00020	AA00120		ADSL – up to 1.5 Mbps download	Circuit	ICB
AA00021	AA00121		ADSL – up to 5 Mbps download	Circuit	ICB
AA00022	AA00122		ADSL – up to 8 Mbps download	Circuit	ICB
Ethernet Access					
AA00201	AA00301		Dedicated Ethernet 1 Mbps	Circuit	
AA00202	AA00302		Dedicated Ethernet 2 Mbps	Circuit	Optional
AA00203	AA00303		Dedicated Ethernet 3 Mbps	Circuit	
AA00204	AA00304		Dedicated Ethernet 5 Mbps	Circuit	Optional
AA00205	AA00305		Dedicated Ethernet 6 Mbps	Circuit	
AA00206	AA00306		Dedicated Ethernet 10 Mbps	Circuit	
AA00207	AA00307		Dedicated Ethernet 20 Mbps	Circuit	Optional
AA00208	AA00308		Dedicated Ethernet 30 Mbps	Circuit	Optional
AA00209	AA00309		Dedicated Ethernet 40 Mbps	Circuit	Optional

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
AA00210	AA00310		Dedicated Ethernet 50 Mbps	Circuit	Optional
AA00211	AA00311		Dedicated Ethernet 60 Mbps	Circuit	Optional
AA00212	AA00312		Dedicated Ethernet 70 Mbps	Circuit	Optional
AA00213	AA00313		Dedicated Ethernet 80 Mbps	Circuit	Optional
AA00214	AA00314		Dedicated Ethernet 90 Mbps	Circuit	Optional
AA00215	AA00315		Dedicated Ethernet 100 Mbps	Circuit	
AA00216	AA00316		Dedicated Ethernet 200 Mbps	Circuit	Optional
AA00217	AA00317		Dedicated Ethernet 300 Mbps	Circuit	Optional
AA00218	AA00318		Dedicated Ethernet 400 Mbps	Circuit	Optional
AA00219	AA00319		Dedicated Ethernet 500 Mbps	Circuit	Optional
AA00220	AA00320		Dedicated Ethernet 600 Mbps	Circuit	Optional
AA00221	AA00321		Dedicated Ethernet 700 Mbps	Circuit	Optional
AA00222	AA00322		Dedicated Ethernet 800 Mbps	Circuit	Optional
AA00223	AA00323		Dedicated Ethernet 900 Mbps	Circuit	Optional
AA00224	AA00324		Dedicated Ethernet 1 Gbps	Circuit	
AA00225	AA00325		Dedicated Ethernet 10 Gbps	Circuit	Optional
AA00226	AA00326		Dedicated Ethernet 20 Gbps	Circuit	Optional; ICB
AA00227	AA00327		Dedicated Ethernet 30 Gbps	Circuit	Optional; ICB
AA00228	AA00328		Dedicated Ethernet 40 Gbps	Circuit	Optional; ICB
AA00401	AA00501		Shared Ethernet 1 Mbps	Circuit	
AA00402	AA00502		Shared Ethernet 2 Mbps	Circuit	
AA00403	AA00503		Shared Ethernet 3 Mbps	Circuit	
AA00404	AA00504		Shared Ethernet 5 Mbps	Circuit	
AA00405	AA00505		Shared Ethernet 6 Mbps	Circuit	
AA00406	AA00506		Shared Ethernet 10 Mbps	Circuit	
AA00407	AA00507		Shared Ethernet 20 Mbps	Circuit	
AA00408	AA00508		Shared Ethernet 30 Mbps	Circuit	
AA00409	AA00509		Shared Ethernet 40 Mbps	Circuit	
AA00410	AA00510		Shared Ethernet 50 Mbps	Circuit	
AA00411	AA00511		Shared Ethernet 60 Mbps	Circuit	
AA00412	AA00512		Shared Ethernet 70 Mbps	Circuit	

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
AA00413	AA00513		Shared Ethernet 80 Mbps	Circuit	
AA00414	AA00514		Shared Ethernet 90 Mbps	Circuit	
AA00415	AA00515		Shared Ethernet 100 Mbps	Circuit	
AA00416	AA00516		Shared Ethernet 200 Mbps	Circuit	
AA00417	AA00517		Shared Ethernet 300 Mbps	Circuit	
AA00418	AA00518		Shared Ethernet 400 Mbps	Circuit	
AA00419	AA00519		Shared Ethernet 500 Mbps	Circuit	
AA00420	AA00520		Shared Ethernet 600 Mbps	Circuit	
AA00421	AA00521		Shared Ethernet 700 Mbps	Circuit	
AA00422	AA00522		Shared Ethernet 800 Mbps	Circuit	
AA00423	AA00523		Shared Ethernet 900 Mbps	Circuit	
AA00424	AA00524		Shared Ethernet 1 Gbps	Circuit	
AA00425	AA00525		Shared Ethernet 2 Gbps	Circuit	Optional
AA00426	AA00526		Shared Ethernet 3 Gbps	Circuit	Optional
AA00427	AA00527		Shared Ethernet 4 Gbps	Circuit	Optional
AA00428	AA00528		Shared Ethernet 5 Gbps	Circuit	Optional
AA00429	AA00529		Shared Ethernet 6 Gbps	Circuit	Optional
AA00430	AA00530		Shared Ethernet 7 Gbps	Circuit	Optional
AA00431	AA00531		Shared Ethernet 8 Gbps	Circuit	Optional
AA00432	AA00532		Shared Ethernet 9 Gbps	Circuit	Optional
AA00433	AA00533		Shared Ethernet 10 Gbps	Circuit	Optional
AA00434	AA00534		Shared Ethernet 20 Gbps	Circuit	Optional; ICB
AA00435	AA00535		Shared Ethernet 30 Gbps	Circuit	Optional; ICB
AA00436	AA00536		Shared Ethernet 40 Gbps	Circuit	Optional; ICB
AA00801	AA00901		Shared Ethernet Access 3 Mbps committed, scalable to 10 Mbps	Circuit	
AA00802	AA00902		Shared Ethernet Access 6 Mbps committed, scalable to 10 Mbps	Circuit	
AA00803	AA00903		Shared Ethernet Access 20 Mbps committed, scalable to 100 Mbps	Circuit	
AA00804	AA00904		Shared Ethernet Access 30 Mbps committed, scalable to 100 Mbps	Circuit	
AA00805	AA00905		Shared Ethernet Access 50 Mbps committed, scalable to 100 Mbps	Circuit	
AA00806	AA00906		Shared Ethernet Access 200 Mbps committed, scalable to 1 Gbps	Circuit	

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
AA00807	AA00907		Shared Ethernet Access 300 Mbps committed, scalable to 1 Gbps	Circuit	
AA00808	AA00908		Shared Ethernet Access 2 Gbps committed, scalable to 10 Gbps	Circuit	Optional
AA00809	AA00909		Shared Ethernet Access 3 Gbps committed, scalable to 10 Gbps	Circuit	Optional
		AA00920	Ethernet Access Bandwidth-on-Demand temporary bandwidth increase of 1 Mbps per day; 1 Mbps ≤ committed bandwidth < 10 Mbps	Mbps per day	Requires scalable Ethernet Access circuit
		AA00921	Ethernet Access Bandwidth-on-Demand temporary bandwidth increase of 10 Mbps per day; 10 Mbps ≤ committed bandwidth < 100 Mbps	10 Mbps per day	Requires scalable Ethernet Access circuit
		AA00922	Ethernet Access Bandwidth-on-Demand temporary bandwidth increase of 100 Mbps per day; 100 Mbps ≤ committed bandwidth < 1 Gbps	100 Mbps per day	Requires scalable Ethernet Access circuit
		AA00923	Ethernet Access Bandwidth-on-Demand temporary bandwidth increase of 1 Gbps per day; 1 Gbps ≤ committed bandwidth < 10 Gbps	Gbps per day	Optional. Requires scalable Ethernet Access circuit
AA00930			Expedited provisioning of Ethernet Access within 24 hours	Circuit	
Cable Access (Download/Upload)					
AA01001	AA01101		Cable Access (5 Mbps / 1 Mbps)	Connection	Optional
AA01002	AA01102		Cable Access (10 Mbps / 1 Mbps)	Connection	Optional
AA01003	AA01103		Cable Access (20 Mbps / 2 Mbps)	Connection	Optional
AA01004	AA01104		Cable Access (30 Mbps / 5 Mbps)	Connection	Optional
FTTP Access					
AA01201	AA01301		FTTP (5 Mbps downstream, 2 Mbps upstream)	Connection	Optional
AA01202	AA01302		FTTP (15 Mbps downstream, 2 Mbps upstream)	Connection	Optional
AA01203	AA01303		FTTP (30 Mbps downstream, 5 Mbps upstream)	Connection	Optional
Wireless Access					
AA01401	AA01501		Broadband Wireless DS1	Link*	ICB
AA01402	AA01502		Broadband Wireless DS3	Link*	ICB
AA01403	AA01503		Broadband Wireless OC-3	Link*	ICB
AA01404	AA01504		Broadband Wireless E1	Link*	ICB. Non-domestic only
AA01405	AA01505		Broadband Wireless E3	Link*	ICB. Non-domestic only

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
AA01406	AA01506		Broadband Wireless 1 Gbps	Link*	ICB
AA01407	AA01507		Broadband Wireless 5 Gbps	Link*	ICB
AA01408	AA01508		Broadband Wireless 10 Gbps	Link*	ICB

* Link is defined as a line-of-sight connection, or one hop, using licensed frequencies

Tables B.2.9.1.6 and B.2.9.1.7 provide the format for pricing information for Access Diversity and Avoidance Prices. Alternate PCL and POP data shall be included in the price table where applicable.

B.2.9.1.6 Access Diversity and Avoidance Prices Table

CLIN	Case Number*	Task Order Number	NSC	Primary PCL**	Price	Alternate PCL***	Alternate POP***	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** PCLs are defined in B.4.1.5
*** Where applicable

B.2.9.1.7 Access Diversity and Avoidance Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
AA01601	AA01701	Access Route or Path Diversity - Alternate PCL	Circuit	ICB. List both primary and alternate PCL
AA01602	AA01702	Access Route or Path Diversity - Alternate POP	Circuit	ICB. List primary PCL and alternate POP
AA01603	AA01703	Access Route or Path Diversity - Alternate PCL and POP	Circuit	ICB. List both primary and alternate PCL and alternate POP
AA01604	AA01704	Access Route or Path Avoidance	Circuit	ICB. List alternate PCL and POP where applicable

Special Access Construction may be required when certain conditions are applicable. See Section C.2.9.1.1 for a list of those conditions and the technical requirements. Tables B.2.9.1.8 and B.2.9.1.9 provide the pricing format.

Special Access Construction prices shall not be applicable to provision a circuit ordered by the CLINs in Table B.2.9.1.5 if:

1. A domestic building NSC is mapped to a PHub ID in Table B.4.1.7 for which a price exists on contract in Table B.2.9.1.1, or
2. A non-domestic price exists for the NSC/CLIN combination in Table B.2.9.1.1~~B.2.9.1.2~~

unless the contractor proves that sufficient capacity is not available solely for the Government.

For each ICB Special Access Construction price, the contractor shall perform a Site Survey and shall provide a Site Survey Estimate with the TO proposals or as specified in each TO. Site Surveys for Special Access Construction are priced under Cable and Wiring in Table B.2.12.1. The estimate must include sufficient information to establish that the special construction price is fair and reasonable. Section J.10 includes a Site Survey Estimate Template for Special Access Construction that identifies the type of data required.

B.2.9.1.8 Special Access Construction Prices Table

CLIN	Case Number	Task Order Number	NSC	PCL*	Price	Price Start Date	Price Stop Date

* PCLs are defined in B.4.1.5~~B.4.1.5~~

B.2.9.1.9 Special Access Construction Pricing Instructions Table

NRC CLIN	Description	Charging Unit	Notes
AA01801	Special Access Construction	ICB	ICB

Tables B.2.9.1.10 and B.2.9.1.11 provide the format for pricing information for the features available with the access arrangement.

B.2.9.1.10 Access Feature Prices Table

CLIN	Case Number	Task Order Number	Country/Jurisdiction ID*	Price	Price Start Date	Price Stop Date

* Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.9.1.11 Access Feature Pricing Instructions Table

NRC CLIN	MRC CLIN	Description	Charging Unit	Notes
AA02001	AA02101	Channelized or Non-Concatenated Access Circuit	Circuit	NSP. Contractor shall use this CLIN to indicate that a channelized or non-concatenated circuit is being ordered (instead of un-channelized or concatenated) at no additional cost

B.2.9.1.12 Access Arrangement Task Order Unique CLINs

Table B.2.9.1.12.1 provides the format for pricing TUCs supported by AA. Table B.2.9.1.12.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.9.1.12.1 Access Arrangement TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.9.1.12.2 Access Arrangement TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
AA99990	AA99991	AA99992	Access Arrangement Task Order Unique	ICB	ICB

B.2.10 Service Related Equipment

The technical requirements for Service Related Equipment (SRE) are defined in Section C.2.10.

Unless otherwise specifically agreed to by the government, all equipment (hardware, firmware, and software) needed on the contractor's side of the demarcation to provide a service is part of the service and shall not be separately priced as SRE.

B.2.10.1 Definition and Online Catalog Requirement

SRE refers to separately identifiable and separately priced hardware, firmware, and software components, along with the installation, maintenance, relocation and/or removal associated with an EIS service.

SRE shall be ancillary to services acquired under this contract.

The contractor shall develop and maintain an online catalog of SRE offerings and pricing in accordance with the requirements specified in Section B.1.3.

The SRE Catalog provided by the contractor shall, at a minimum, contain the data elements defined in this section. In addition, the contractor shall list, where available, the month and year of model introduction, provide references to this information on its websites, or indicate how to find this information on the manufacturer's website. If the model introduction date is unavailable, or is an estimate, then the contractor shall indicate this in its catalog. Other information may be provided by the contractor in its catalog at its option.

B.2.10.2 Catalog Requirements for Pricing Information

SRE NRC prices shall be based on a discount from the Official List Price (OLP) as described in this section. The SRE OLP shall be the manufacturer's OLP. The contractor shall identify the trade name(s) for the OLP (e.g., MSRP, OEM list price). The information needed to determine a single discounted CONUS NRC shall be included in the contractor's SRE Catalog as defined in Tables B.2.10.2.1 and B.2.10.2.2 below. Charging mechanisms are defined in Table B.2.10.2.3.

B.2.10.2.1 SRE Catalog – Product Specification Table

CLIN	Case Number	SRE Type	Manufacturer	Model No.	Part No.	UPC	Model/Part Description	Device Size	Rated for Energy Efficiency Compliance	Energy Efficiency Standards and Ratings	OLP	No List Price	Device Class ID	SRE MRC Options	Start Date	Stop Date	End of Sale Date	End of Life Date	Notes
		S, B, C, or A							*Y/N*				*(From Table B.2.10.2.2~~B.2.10.2.2~~)*						

Table notes:

1. SRE Type: S (stand-alone), B (base unit), C (configurable component), or A (accessory) - see definitions in Section B.2.10.5~~B.2.10.5~~.
2. SRE model numbers and SRE part numbers shall be specified by the contractor. Where a model number is not available, insert "N/A". Part number shall be the manufacturer's part number.
3. For each unique case number, the combination of Manufacturer+Model No.+Part No. shall be unique.
4. SRE descriptions shall be sufficiently complete that all capabilities and limitations of the SRE, as priced, are clear to the government.
5. Device Size: a numerical value from 1 to 5 representing the size of the SRE for device management purposes (see Section B.2.8.1.3): 1=extra small, 2=small, 3=medium, 4=large, 5=extra large
6. Energy Efficiency Standards and Ratings: The contractor shall itemize all energy efficiency ratings such as FEMP, EPEAT, Energy Star, etc. in this column.
7. No List Price: "T" if the price appearing in the OLP column is not an official list price, "F" otherwise.
8. SRE MRC Options: null for SRE Type A, otherwise an array value containing the monthly payment options being offered from the set {12, 24, 36, 48}.
9. End of Sale Date shall be the effective date after which an item may no longer be purchased. Stop Date shall not be later than End of Sale Date.
10. End of Life Date shall be the effective date after which an item is no longer supported by the contractor.

The discount to be applied to the OLP is determined by the Device Class ID. The device class elements are shown in Table B.2.10.2.2. The SRE NRC shall be the OLP less the discount for the device class.

B.2.10.2.2 SRE Device Class Discount Table

Device Class ID*	Device Class Description**	Task Order Number	Percentage Discount from OLP**	Start Date	Stop Date
6000					
…					
6999					

* The number of device classes shall be selected by the contractor from within the range shown
** The Device Class Description and the Percentage Discount for each device class shall be constant and fixed through the life of the contract, unless changed by contract modification (the Start and Stop Dates shall only apply when a change is caused by contract modification).

If the OLP is not available for a particular SRE, the SRE NRC shall be agreed upon between the contractor and the ordering agency at time of TO award. In Table B.2.10.2.1, the contractor shall populate the OLP column with the agreed upon price, populate the No List Price column with “T”, and specify a device class having a discount of zero. Other price elements shall be provided as appropriate and available.

B.2.10.2.3 SRE Instruction Table

CLIN	Frequency	Description	Charging Unit	Notes
EQ90001	NRC	SRE Catalog Item	ICB	ICB

B.2.10.3 Specific Catalog Requirements for SRE Pricing

The contractor’s catalog shall include some or all of the following SRE pricing elements:

- An NRC for initial installation and outside moves of SRE connected at a fixed location. The installation NRC is not applicable for Configurable Component SRE.
- An NRC for inside moves of SRE at a fixed location (i.e., an equipment move within same premises without change of the access arrangement). The inside move NRC is not applicable for Configurable Component or Accessory SRE.
- An NRC for on-site modification or upgrade of installed equipment at a fixed location. For a mobile SRE, this pricing element shall apply for an off-site modification or upgrade of delivered equipment, including all associated transportation costs associated with drop-off and return. The upgrade NRC for a Base Unit of a Packaged SRE includes the subsequent installation of one or

more Configurable Components at the same time for an already installed Base Unit. The upgrade NRC is not applicable for Configurable Component or Accessory SRE.

- A monthly maintenance charge (MMC) for ongoing maintenance, starting with the accepted installation or completed delivery of the SRE. The upgrade or modification of SRE that is a patch, reload, replacement, add-on, or adjustment to remove design, manufacturing, or programming defects or faults; remove unexpected security liabilities; effect compatibility with formalized standards, or other similar actions of the type typically recommended by the manufacturer to assure optimal performance, shall be part of normal SRE maintenance, is covered by the MMC, and shall not be subject to an additional NRC.
- SRE MRCs for an indeterminate month-to month MRC or for fixed durations of 24, 36, or 48 months. The agency will select either an SRE NRC or SRE MRC and duration at time of order. At the end of the contract, all SRE MRCs terminate regardless of any remaining months in the selected time period.

Reference Table B.2.10.3.1 shows the pricing elements that shall be provided with each SRE included in the contractor's SRE Catalog. Additional pricing elements may be defined upon request by the contractor.

B.2.10.3.1 SRE Pricing Elements Reference

SRE Pricing Element	Description of SRE Pricing Element	Frequency	Calculated Price
1	SRE NRC	NRC	T
2	Installation NRC	NRC	F
3	Monthly Maintenance Charge (MMC)	MRC	F
4	Inside Move NRC	NRC	F
5	Upgrade NRC	NRC	F
12	Month-to-Month MRC	MRC	T
24	24-Month Installment MRC	MRC	T
36	36-Month Installment MRC	MRC	T
48	48-Month Installment MRC	MRC	T

Table B.2.10.3.2 shows the information that shall be provided to price each SRE pricing element identified for a given SRE in the contractor's catalog. The contractor shall use Table B.2.10.3.2 to price only those pricing elements from Table B.2.10.3.1 where the Calculated Price="F". Pricing elements where the Calculated Price="T" in Table

B.2.10.3.1 shall not be priced by the contractor in Table B.2.10.3.2 but instead will be calculated by the government.

B.2.10.3.2 SRE Catalog Prices Table

CLIN	Case Number	SRE Pricing Element	Task Order Number	AOW ID	Price	Price Start Date	Price Stop Date
(from Table B.2.10.2.1 ~~B.2.10.2.1~~)	*(from Table B.2.10.2.1 ~~B.2.10.2.1~~)*	*(integer value from Table B.2.10.3.1~~B.2.10.3.1~~)*		*(from Table B.2.10.10.1 ~~B.2.10.10.1~~)*			

Formatte
Formatte
Formatte
Formatte

De-installation of contractor-owned SRE installed on the customer's premises, including storage, packaging for shipment, and/or transportation, shall be provided by the contractor at no additional charge to the government. For end-user mobile devices such as phones and tablets, de-installation means arranging for return of the device to the contractor at no additional charge to the government.

B.2.10.4 Payment Methods

The contractor shall offer the government a choice of two methods to pay for use of each SRE. The government will decide which payment method to select at the time of order.

1. (SRE Pricing Element 1) One-time charge for use of SRE paid in a single installment, the SRE NRC.
2. (SRE Pricing Elements 12, 24, 36, and 48) Equal monthly SRE MRC installments for an indeterminate term month-to-month arrangement, or for a fixed designated period of either 24, 36, or 48 months, as defined by the contractor for a particular SRE, starting once service has been accepted by the user agency. The SRE MRC charges shall be computed by dividing the SRE NRC by the designated period (month-to-month shall use 12 as the designated period), and multiplying by the appropriate Monthly Payment Factor from Table B.2.10.4.1.

B.2.10.4.1 SRE Monthly Payment Factor Table

SRE Pricing Element	Cost-of-Money Percent (rate per annum)*	Margin Percent**	Monthly Payment Percent***	Monthly Payment Factor****	Start Date	Stop Date
12						
24						
36						

SRE Pricing Element	Cost-of-Money Percent (rate per annum)*	Margin Percent**	Monthly Payment Percent***	Monthly Payment Factor****	Start Date	Stop Date
48						

* Cost-of-Money Percent will be populated by the government and will remain constant for a six-month period
** Margin Percent shall be specified by the contractor and remain constant for the life of the contract
*** Monthly Payment Percent shall be equal to (Cost-of-Money Percent + Margin Percent)
**** Monthly Payment Factor shall be equal to 100% + Monthly Payment Percent, converted to decimal format (e.g., 100% + 4% = 104%= 1.04)

The Cost-of-Money Percent for SRE MRC shall be based on the floating index rate specified below. The floating index rate shall be the monthly average yield, as established every six months, in percent per annum on Treasury securities adjusted to constant maturities. The monthly index rate used shall be the rate published in the Federal Reserve Statistical Release H.15 on the first business day of January and the first business day of July of each year. This index rate shall be in effect on a semiannual basis, from the fifteenth of the month in which it is published to the fourteenth of the following sixth month. For orders that use SRE MRC for a device, the index rate used to compute the cost of money factor shall be the index rate in effect on the date the order is issued. Where the order is for a rental period (e.g., 48 months) different from the periods listed for Treasury securities (e.g., 2, 3, and 5 years) in H.15, the index rate used shall be the rate available for the next longer period (e.g., 5 years).

SRE NRC and its associated SRE MRCs shall be those that are in effect at the time a particular SRE is ordered (i.e., the price of the SRE is the price in effect on the completion date on the SOCN). This price shall apply throughout the in-service life of the ordered SRE, irrespective of subsequent price changes for that SRE NRC and its associated SRE MRC(s) shown in the contractor catalog. This requirement does not apply to SRE NRCs for moves and changes, or to the MMC.

If an SRE MRC period selected by a user is terminated by the user before the period has concluded (for the purpose of having SRE removed by the contractor), in addition to all applicable SRE MRCs due up to the notice of termination, a refurbishment payment equal to 25% of the remaining projected payments due for the selected SRE MRC term period shall apply. However, in no case shall the amount of the refurbishment payment exceed the SRE NRC. If a user initially selects an SRE MRC payment term, and subsequently chooses to terminate its SRE MRC payment term early and continue using the associated SRE, the user shall pay the SRE NRC, less the cumulative SRE MRC payments (exclusive of finance charges defined by the Monthly Payment Factor) paid up to the time of notification of such selection.

Table B.2.10.4.2 provides the format for pricing SRE MRC early termination and Table B.2.10.4.3 provides the charging mechanisms.

B.2.10.4.2 SRE MRC Term Period Early Termination Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.10.4.3 SRE MRC Term Period Early Termination Pricing Instructions Table

NRC CLIN	Description	Charging Unit	Notes
EQ99998	SRE MRC term period early termination with removal of SRE by contractor	ICB	ICB
EQ99999	SRE MRC term period early termination with continued use of SRE by user	ICB	ICB

Because all SRE MRC payments automatically cease on the end date of this contract, the contractor may decline to provide SRE MRC term periods that are longer than the then-remaining maximum potential term of the contract. If the contract is terminated for convenience, or the government elects not to exercise an option period, any active SRE MRC term periods for SRE cut short by such an event shall be subject to the same rules that would apply for a user-requested early termination of a SRE MRC term.

The payment method for a separately priced, additional configurable component element in a packaged SRE shall be consistent with that selected for the base unit, except when an additional configurable component is added to a base unit after the initial installation/delivery of the packaged unit has been accepted by the user. The payment method for an accessory shall be to pay for it in a single installment (SRE NRC). When a user selects the single installment payment method for a packaged unit, the single installment price shall include the SRE NRCs of all components of the fully functional packaged unit at time of its installation/delivery.

In certain cases, orders may be renewed annually due to the type of funding used. The government's commitment on order renewal may be limited by funds availability.

B.2.10.5 Pricing Types

SRE pricing shall allow for multiple SRE types. Some types are stand-alone self-sufficient units that include all needed SRE functions for that type, while others are

component based and may be configured in a variety of ways to offer different functionality. The following SRE types may be priced separately:

- Stand-alone units
- Packaged units consisting of one or more of the following:
  - Base units of packaged SRE
  - Configurable components
- Accessories

B.2.10.5.1 Stand-Alone Unit

An SRE stand-alone unit is a self-contained, fully functioning device (e.g., a CSU/DSU or handset). No separately-priced plug-in, attachable, or loadable components to modify or upgrade its performance or essential functionality are provided. Each stand-alone SRE unit shall be separately priced.

B.2.10.5.2 Packaged Unit

A SRE packaged unit consists of a package of component elements including a separately-priced "base unit" (containing all minimally-required elements) and a variable list of separately-priced additional configurable components. Examples of packaged units include routers, smart multiplexers, and Very Small Aperture Terminals (VSATs).

B.2.10.5.2.1 Base Unit

The SRE base unit shall include only those underlying base components that are needed to support the common or shared functions of the equipment before the addition of the configurable components. Accordingly, the SRE base unit price shall include common use components such as chassis, shelves, interconnecting and power cables, internal power supply(s), mounting fixtures, antenna, CPU and the hardware and firmware/software components of basic memory and operating system, as applicable.

B.2.10.5.2.2 Configurable Components

Configurable components are those separately-priced components needed to equip the base unit of packaged SRE for a specific billed user at the service location.

Such configurable components shall include the plug-in, attachable, or loadable items such as line, circuit, network, and feature cards/blades, memory and/or operating system upgrades, and other firmware or software items needed to configure the base unit so that it can fully implement the required functionality of the packaged SRE. Additional components may be added separately to upgrade or modify a previously installed packaged unit.

B.2.10.5.3 Accessories

Accessories enhance the use of a device, but are not needed to implement the essential function(s) of the device (e.g., a spare battery or carrying case for a cellular/ mobile satellite device, or an additional copy of a user manual).

B.2.10.6 Monthly Maintenance Charges

An MMC shall apply to each installed/delivered stand-alone SRE unit and/or each installed/delivered base unit of a packaged SRE unit. The ongoing MMC shall cover all maintenance/repair costs for the SRE during its installed life, and shall include the stocking of needed maintenance spares, and any necessary hardware, firmware, and software upgrades required to maintain its functionality and usability during its supported life.

MMC shall not be permitted for the separately-priced additional individual configurable components of a packaged SRE unit or for SRE accessories, except where such components have an OLP equal to or greater than $5,000.

B.2.10.7 Wireless SRE Termination of Support

For wireless mobile devices only, the notice period for termination of support described in Section B.1.3.3 shall be at least 30 days prior to when the contractor no longer offers a particular device. For wireless mobile device accessories only, the notice period for termination of support described in Section B.1.3.3 shall be at least 120 days prior to when the contractor no longer offers a particular accessory or its equivalent.

B.2.10.8 Government Option to Assume Ownership

The government may, at its sole discretion, following payment of the SRE NRC or at completion of the SRE MRC payment term, assume ownership of the SRE, as described in FAR 52.207-5. When the government has assumed ownership of SRE, the user will have the option to continue receiving maintenance from the contractor. In this case, the contractor shall provide the same level of maintenance at the MMC established for the SRE when it was contractor-owned. Continued support following a change in ownership is subject to the termination of support provision in Section B.2.10.7.

B.2.10.9 Abandonment

Unless otherwise agreed to by the user, the contractor shall not abandon or otherwise leave behind contractor-provided and contractor-owned equipment that was installed at a user site and that is no longer invoiced, either during the term of the contract or at end of contract. Such fixed location equipment shall be removed within 45 days after the last

effective billing period, or within 10 business days following a formal government request. This provision shall not apply to unbilled maintenance spares in place in support of billed equipment at the same site or to in-place equipment that is in the process of change of ownership pursuant to B.2.10.8.

B.2.10.10 Area of the World Price Adjustment Factor

SRE pricing may be adjusted to reflect certain cost differentials associated with provision of SRE at OCONUS and Non-Domestic locations. Pricing may be adjusted by use of a factor applied to the CONUS catalog prices. These factors may be applied, for example, when a foreign government requires an item needed under this contract to be manufactured or purchased within its country.

Area of the world (AOW) price adjustments shall be identified and specified in the contractor's catalog in accordance with the AOW price adjustment factors. These factors may be "1" or greater or less than "1". The CONUS factor shall be 1.0. The contractor shall specify an AOW price adjustment factor for each Area of the World in Table B.2.10.10.1 below where the contractor offers SRE in at least one of the Country/Jurisdictions contained in that AOW. The correlation of an AOW ID with a particular Country/Jurisdiction ID is provided in Table B.4.2.1.

B.2.10.10.1 Area of the World Price Adjustment Factor

Area of the World (AOW)	AOW ID	AOW Price Adjustment Factor*	Start Date	Stop Date
CONUS	200000	1.0		
Alaska, Guam, Hawaii, Puerto Rico, and USVI (OCONUS)	200001			
American Samoa, CNMI, Marshall Islands, Micronesia, Palau, Midway Island, and Wake Island (OCONUS)	200002			
Canada, Mexico, and Bermuda	200003			
Central, South America, and the Caribbean	200004			
Europe (Western & Eastern Europe)	200005			
Middle East (including Egypt and Turkey)	200006			
Russia and Eurasian Area	200007			
Japan, the Philippines, South Korea, and Taiwan	200008			
Rest of Asia (North, South, and Southeast Asia)	200009			
Australia / New Zealand	200010			
Northern Africa	200011			
Sub-Saharan Africa	200012			

Area of the World (AOW)	AOW ID	AOW Price Adjustment Factor*	Start Date	Stop Date
Antarctica	200013			
Rest of World	200014			

* Factors shall be constant and fixed through the life of the contract unless changed by contract modification (the Start and Stop dates shall only apply to a change of price adjustment factor caused by contract modification). For each row of the table, the initial Start Date shall be the contract award date, and the initial Stop Date shall be the contract termination date.

B.2.11 Service Related Labor

B.2.11.1 Labor Service

The technical requirements for Service Related Labor are described in Section C.2.11.

Labor service performed under this contract shall be on a time and materials or firm fixed price basis.

B.2.11.2 Labor Categories

The labor categories included in this contract are described in Section J.5.

For each labor category in this contract, Table B.2.11.7.2 indicates the applicable Bureau of Labor Statistics Standard Occupational Classification (BLS-SOC) O*NET code and the occupational group index that will be applied to escalate labor rates for that labor category.

Labor categories are further subdivided into three levels: Junior, Journeyman, and Senior / Subject Matter Expert (SME), based on years of experience and duties/responsibilities as follows:

- JUNIOR: An individual in the Junior labor category level has up to 3 years of applicable experience. Such an individual is responsible for assisting more senior positions and/or performing functional duties under the oversight of more senior positions.
- JOURNEYMAN: An individual in the Journeyman labor category level has 3 to 10 years of applicable experience. Such an individual typically performs all functional duties independently.
- SENIOR/SME: An individual in the Senior / Subject Matter Expert (SME) labor category has more than 10 years of applicable experience, or is an individual whose qualifications or expertise are exceptional, or is recognized as an industry

leader for a given area of expertise. Such an individual performs all functional duties independently, and may oversee the efforts of less senior staff and/or be responsible for the efforts of all staff assigned to a specific job.

B.2.11.3 CONUS Pricing

The contractor shall propose fixed, fully-loaded prices for the labor categories specified in Section J.5 for CONUS (see Section J.12 for definitions of CONUS, OCONUS and Non-Domestic).

For each labor category, the contractor shall propose an on-site (i.e., on government premises) and an off-site (i.e., on contractor premises) price, in two separate CLINs. The contract prices shall stay in effect for the duration of the contract or until contract modifications have been executed to delete or update the prices. Prices provided in the Service Related Labor tables shall be maximum hourly rates for any location in CONUS during normal business hours.

B.2.11.4 Other than CONUS Pricing

The contractor shall provide pricing for OCONUS and Non-Domestic locations only at the TO level.

The U.S. Department of State's Bureau of Administration, Office of Allowances, publishes quarterly report indexes of living costs abroad, per-diem rate maximums, quarter's allowances, hardship differentials, and danger pay allowances.

The Department of State Standardized Regulations (DSSR) control the allowances and benefits available to all U.S. Government civilians assigned to foreign areas. For TOs issued under this contract, civilians employed by the contractor who are assigned to foreign areas may receive the allowances and benefits in the DSSR, but shall not receive allowances and benefits in excess of those identified in the DSSR.

B.2.11.5 Travel

Travel costs may be firm fixed price or reimbursed at actual cost in accordance with the limitations set forth in FAR 31.205-46 and in applicable agency-specific regulatory supplements. Travel costs shall be priced in Table B.2.11.7.3.1 using a Service Related Labor TUC.

B.2.11.6 Materials

Materials are defined and priced in accordance with FAR 16.601. Material costs shall be priced in Table B.2.11.7.3.1 using a Service Related Labor TUC.

B.2.11.7 Service Related Labor Price Structure

Pricing for Service Related Labor shall include the maximum hourly rate for each CLIN.

B.2.11.7.1 Service Related Labor Prices Table

CLIN*	Case Number**	Task Order Number	Country/Jurisdiction ID***	Max Hourly Rate	Rate Start Date	Rate Stop Date

* CLINs are listed in Table B.2.11.7.2
** Applies only to ICB CLINs
*** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.11.7.2 Service Related Labor Pricing Instructions Table

CLIN	Labor Category	BLS-SOC O*NET Code	Occupational Group	Level	Site (G or C)	Frequency	Charging Unit
LA00001	Business Continuity Planner	13-1199.04	Professional and related	Junior	G	Usage	Hour
LA00002	Business Continuity Planner	13-1199.04	Professional and related	Journeyman	G	Usage	Hour
LA00003	Business Continuity Planner	13-1199.04	Professional and related	Senior/SME	G	Usage	Hour
LA00004	Business Continuity Planner	13-1199.04	Professional and related	Junior	C	Usage	Hour
LA00005	Business Continuity Planner	13-1199.04	Professional and related	Journeyman	C	Usage	Hour
LA00006	Business Continuity Planner	13-1199.04	Professional and related	Senior/SME	C	Usage	Hour
LA00007	Computer Network Architect	15-1143.00	Professional and related	Junior	G	Usage	Hour
LA00008	Computer Network Architect	15-1143.00	Professional and related	Journeyman	G	Usage	Hour
LA00009	Computer Network Architect	15-1143.00	Professional and related	Senior/SME	G	Usage	Hour
LA00010	Computer Network Architect	15-1143.00	Professional and related	Junior	C	Usage	Hour

CLIN	Labor Category	BLS-SOC O*NET Code	Occupational Group	Level	Site (G or C)	Frequency	Charging Unit
LA00011	Computer Network Architect	15-1143.00	Professional and related	Journeyman	C	Usage	Hour
LA00012	Computer Network Architect	15-1143.00	Professional and related	Senior/SME	C	Usage	Hour
LA00013	Computer Network Support Specialist	15-1152.00	Professional and related	Junior	G	Usage	Hour
LA00014	Computer Network Support Specialist	15-1152.00	Professional and related	Journeyman	G	Usage	Hour
LA00015	Computer Network Support Specialist	15-1152.00	Professional and related	Senior/SME	G	Usage	Hour
LA00016	Computer Network Support Specialist	15-1152.00	Professional and related	Junior	C	Usage	Hour
LA00017	Computer Network Support Specialist	15-1152.00	Professional and related	Journeyman	C	Usage	Hour
LA00018	Computer Network Support Specialist	15-1152.00	Professional and related	Senior/SME	C	Usage	Hour
LA00019	Computer Systems Analyst	15-1121.00	Professional and related	Junior	G	Usage	Hour
LA00020	Computer Systems Analyst	15-1121.00	Professional and related	Journeyman	G	Usage	Hour
LA00021	Computer Systems Analyst	15-1121.00	Professional and related	Senior/SME	G	Usage	Hour
LA00022	Computer Systems Analyst	15-1121.00	Professional and related	Junior	C	Usage	Hour
LA00023	Computer Systems Analyst	15-1121.00	Professional and related	Journeyman	C	Usage	Hour
LA00024	Computer Systems Analyst	15-1121.00	Professional and related	Senior/SME	C	Usage	Hour

CLIN	Labor Category	BLS-SOC O*NET Code	Occupational Group	Level	Site (G or C)	Frequency	Charging Unit
LA00025	Computer Systems Engineers/ Architect	15-1199.02	Professional and related	Junior	G	Usage	Hour
LA00026	Computer Systems Engineers/ Architect	15-1199.02	Professional and related	Journeyman	G	Usage	Hour
LA00027	Computer Systems Engineers/ Architect	15-1199.02	Professional and related	Senior/SME	G	Usage	Hour
LA00028	Computer Systems Engineers/ Architect	15-1199.02	Professional and related	Junior	C	Usage	Hour
LA00029	Computer Systems Engineers/ Architect	15-1199.02	Professional and related	Journeyman	C	Usage	Hour
LA00030	Computer Systems Engineers/ Architect	15-1199.02	Professional and related	Senior/SME	C	Usage	Hour
LA00031	Customer Service Representative	43-4051.00	Service Occupations	Junior	G	Usage	Hour
LA00032	Customer Service Representative	43-4051.00	Service Occupations	Journeyman	G	Usage	Hour
LA00033	Customer Service Representative	43-4051.00	Service Occupations	Senior/SME	G	Usage	Hour
LA00034	Customer Service Representative	43-4051.00	Service Occupations	Junior	C	Usage	Hour
LA00035	Customer Service Representative	43-4051.00	Service Occupations	Journeyman	C	Usage	Hour
LA00036	Customer Service Representative	43-4051.00	Service Occupations	Senior/SME	C	Usage	Hour
LA00037	Database Administrator	15-1141.00	Professional and related	Junior	G	Usage	Hour
LA00038	Database Administrator	15-1141.00	Professional and related	Journeyman	G	Usage	Hour
LA00039	Database Administrator	15-1141.00	Professional and related	Senior/SME	G	Usage	Hour

CLIN	Labor Category	BLS-SOC O*NET Code	Occupational Group	Level	Site (G or C)	Frequency	Charging Unit
LA00040	Database Administrator	15-1141.00	Professional and related	Junior	C	Usage	Hour
LA00041	Database Administrator	15-1141.00	Professional and related	Journeyman	C	Usage	Hour
LA00042	Database Administrator	15-1141.00	Professional and related	Senior/SME	C	Usage	Hour
LA00043	Database Architect	15-1199.06	Professional and related	Junior	G	Usage	Hour
LA00044	Database Architect	15-1199.06	Professional and related	Journeyman	G	Usage	Hour
LA00045	Database Architect	15-1199.06	Professional and related	Senior/SME	G	Usage	Hour
LA00046	Database Architect	15-1199.06	Professional and related	Junior	C	Usage	Hour
LA00047	Database Architect	15-1199.06	Professional and related	Journeyman	C	Usage	Hour
LA00048	Database Architect	15-1199.06	Professional and related	Senior/SME	C	Usage	Hour
LA00049	Electrical Drafter – Computer Aided Design (CAD) Operator	17-3012.02	Professional and related	Junior	G	Usage	Hour
LA00050	Electrical Drafter – Computer Aided Design (CAD) Operator	17-3012.02	Professional and related	Journeyman	G	Usage	Hour
LA00051	Electrical Drafter – Computer Aided Design (CAD) Operator	17-3012.02	Professional and related	Senior/SME	G	Usage	Hour
LA00052	Electrical Drafter – Computer Aided Design (CAD) Operator	17-3012.02	Professional and related	Junior	C	Usage	Hour
LA00053	Electrical Drafter – Computer Aided Design (CAD) Operator	17-3012.02	Professional and related	Journeyman	C	Usage	Hour

CLIN	Labor Category	BLS-SOC O*NET Code	Occupational Group	Level	Site (G or C)	Frequency	Charging Unit
LA00054	Electrical Drafter – Computer Aided Design (CAD) Operator	17-3012.02	Professional and related	Senior/SME	C	Usage	Hour
LA00055	Information Security Analyst	15-1122.00	Professional and related	Junior	G	Usage	Hour
LA00056	Information Security Analyst	15-1122.00	Professional and related	Journeyman	G	Usage	Hour
LA00057	Information Security Analyst	15-1122.00	Professional and related	Senior/SME	G	Usage	Hour
LA00058	Information Security Analyst	15-1122.00	Professional and related	Junior	C	Usage	Hour
LA00059	Information Security Analyst	15-1122.00	Professional and related	Journeyman	C	Usage	Hour
LA00060	Information Security Analyst	15-1122.00	Professional and related	Senior/SME	C	Usage	Hour
LA00061	Information Technology Project Manager	15-1199.09	Management, business, and financial	Junior	G	Usage	Hour
LA00062	Information Technology Project Manager	15-1199.09	Management, business, and financial	Journeyman	G	Usage	Hour
LA00063	Information Technology Project Manager	15-1199.09	Management, business, and financial	Senior/SME	G	Usage	Hour
LA00064	Information Technology Project Manager	15-1199.09	Management, business, and financial	Junior	C	Usage	Hour
LA00065	Information Technology Project Manager	15-1199.09	Management, business, and financial	Journeyman	C	Usage	Hour
LA00066	Information Technology Project Manager	15-1199.09	Management, business, and financial	Senior/SME	C	Usage	Hour

CLIN	Labor Category	BLS-SOC O*NET Code	Occupational Group	Level	Site (G or C)	Frequency	Charging Unit
LA00067	Network and Computer Systems Administrator	15-1142.00	Professional and related	Junior	G	Usage	Hour
LA00068	Network and Computer Systems Administrator	15-1142.00	Professional and related	Journeyman	G	Usage	Hour
LA00069	Network and Computer Systems Administrator	15-1142.00	Professional and related	Senior/SME	G	Usage	Hour
LA00070	Network and Computer Systems Administrator	15-1142.00	Professional and related	Junior	C	Usage	Hour
LA00071	Network and Computer Systems Administrator	15-1142.00	Professional and related	Journeyman	C	Usage	Hour
LA00072	Network and Computer Systems Administrator	15-1142.00	Professional and related	Senior/SME	C	Usage	Hour
LA00073	Software Developer–Applications	15-1132.00	Professional and related	Junior	G	Usage	Hour
LA00074	Software Developer – Applications	15-1132.00	Professional and related	Journeyman	G	Usage	Hour
LA00075	Software Developer – Applications	15-1132.00	Professional and related	Senior/SME	G	Usage	Hour
LA00076	Software Developer – Applications	15-1132.00	Professional and related	Junior	C	Usage	Hour
LA00077	Software Developer – Applications	15-1132.00	Professional and related	Journeyman	C	Usage	Hour
LA00078	Software Developer – Applications	15-1132.00	Professional and related	Senior/SME	C	Usage	Hour
LA00079	Software Developer – Systems Software	15-1133.00	Professional and related	Junior	G	Usage	Hour
LA00080	Software Developer – Systems Software	15-1133.00	Professional and related	Journeyman	G	Usage	Hour

CLIN	Labor Category	BLS-SOC O*NET Code	Occupational Group	Level	Site (G or C)	Frequency	Charging Unit
LA00081	Software Developer – Systems Software	15-1133.00	Professional and related	Senior/SME	G	Usage	Hour
LA00082	Software Developer – Systems Software	15-1133.00	Professional and related	Junior	C	Usage	Hour
LA00083	Software Developer – Systems Software	15-1133.00	Professional and related	Journeyman	C	Usage	Hour
LA00084	Software Developer – Systems Software	15-1133.00	Professional and related	Senior/SME	C	Usage	Hour
LA00085	Software Quality Assurance Engineer/ Tester	15-1199.01	Professional and related	Junior	G	Usage	Hour
LA00086	Software Quality Assurance Engineer/ Tester	15-1199.01	Professional and related	Journeyman	G	Usage	Hour
LA00087	Software Quality Assurance Engineer/ Tester	15-1199.01	Professional and related	Senior/SME	G	Usage	Hour
LA00088	Software Quality Assurance Engineer/ Tester	15-1199.01	Professional and related	Junior	C	Usage	Hour
LA00089	Software Quality Assurance Engineer/ Tester	15-1199.01	Professional and related	Journeyman	C	Usage	Hour
LA00090	Software Quality Assurance Engineer/ Tester	15-1199.01	Professional and related	Senior/SME	C	Usage	Hour
LA00091	Sustainability Specialist	13-1199.05	Professional and related	Junior	G	Usage	Per Hour
LA00092	Sustainability Specialist	13-1199.05	Professional and related	Journeyman	G	Usage	Per Hour

CLIN	Labor Category	BLS-SOC O*NET Code	Occupational Group	Level	Site (G or C)	Frequency	Charging Unit
LA00093	Sustainability Specialist	13-1199.05	Professional and related	Senior/SME	G	Usage	Per Hour
LA00094	Sustainability Specialist	13-1199.05	Professional and related	Junior	C	Usage	Per Hour
LA00095	Sustainability Specialist	13-1199.05	Professional and related	Journeyman	C	Usage	Per Hour
LA00096	Sustainability Specialist	13-1199.05	Professional and related	Senior/SME	C	Usage	Per Hour
LA00097	Telecommunications Engineering Specialist	15-1143.01	Professional and related	Junior	G	Usage	Hour
LA00098	Telecommunications Engineering Specialist	15-1143.01	Professional and related	Journeyman	G	Usage	Hour
LA00099	Telecommunications Engineering Specialist	15-1143.01	Professional and related	Senior/SME	G	Usage	Hour
LA00100	Telecommunications Engineering Specialist	15-1143.01	Professional and related	Junior	C	Usage	Hour
LA00101	Telecommunications Engineering Specialist	15-1143.01	Professional and related	Journeyman	C	Usage	Hour
LA00102	Telecommunications Engineering Specialist	15-1143.01	Professional and related	Senior/SME	C	Usage	Hour
LA00103	Telecommunications Equipment Installer/ Repairer	49-2022.00	Service Occupations	Junior	G	Usage	Hour
LA00104	Telecommunications Equipment Installer/ Repairer	49-2022.00	Service Occupations	Journeyman	G	Usage	Hour
LA00105	Telecommunications Equipment Installer/ Repairer	49-2022.00	Service Occupations	Senior/SME	G	Usage	Hour

CLIN	Labor Category	BLS-SOC O*NET Code	Occupational Group	Level	Site (G or C)	Frequency	Charging Unit
LA00106	Telecommunications Equipment Installer/ Repairer	49-2022.00	Service Occupations	Junior	C	Usage	Hour
LA00107	Telecommunications Equipment Installer/ Repairer	49-2022.00	Service Occupations	Journeyman	C	Usage	Hour
LA00108	Telecommunications Equipment Installer/ Repairer	49-2022.00	Service Occupations	Senior/SME	C	Usage	Hour
LA00109	Telecommunications Line Installer/ Repairer	49-9052.00	Service Occupations	Junior	G	Usage	Hour
LA00110	Telecommunications Line Installer/ Repairer	49-9052.00	Service Occupations	Journeyman	G	Usage	Hour
LA00111	Telecommunications Line Installer/ Repairer	49-9052.00	Service Occupations	Senior/SME	G	Usage	Hour
LA00112	Telecommunications Line Installer/ Repairer	49-9052.00	Service Occupations	Junior	C	Usage	Hour
LA00113	Telecommunications Line Installer/ Repairer	49-9052.00	Service Occupations	Journeyman	C	Usage	Hour
LA00114	Telecommunications Line Installer/ Repairer	49-9052.00	Service Occupations	Senior/SME	C	Usage	Hour
LA00115	Web Administrator	15-1199.03	Professional and related	Junior	G	Usage	Hour
LA00116	Web Administrator	15-1199.03	Professional and related	Journeyman	G	Usage	Hour
LA00117	Web Administrator	15-1199.03	Professional and related	Senior/SME	G	Usage	Hour
LA00118	Web Administrator	15-1199.03	Professional and related	Junior	C	Usage	Hour
LA00119	Web Administrator	15-1199.03	Professional and related	Journeyman	C	Usage	Hour

CLIN	Labor Category	BLS-SOC O*NET Code	Occupational Group	Level	Site (G or C)	Frequency	Charging Unit
LA00120	Web Administrator	15-1199.03	Professional and related	Senior/SME	C	Usage	Hour
LA00121	Web Developer	15-1134.00	Professional and related	Junior	G	Usage	Hour
LA00122	Web Developer	15-1134.00	Professional and related	Journeyman	G	Usage	Hour
LA00123	Web Developer	15-1134.00	Professional and related	Senior/SME	G	Usage	Hour
LA00124	Web Developer	15-1134.00	Professional and related	Junior	C	Usage	Hour
LA00125	Web Developer	15-1134.00	Professional and related	Journeyman	C	Usage	Hour
LA00126	Web Developer	15-1134.00	Professional and related	Senior/SME	C	Usage	Hour

B.2.11.7.3 Service Related Labor Task Order Unique CLINs

Table B.2.11.7.3.1 provides the format for pricing TUCs associated with Service Related Labor. Table B.2.11.7.3.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.2.11.7.3.1 Service Related Labor TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.2.11.7.3.2 Service Related Labor TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
LA99990	LA99991	LA99992	Service Related Labor Task Order Unique	ICB	ICB

B.2.12 Cable and Wiring

The technical requirements for Cable and Wiring are defined in Section C.2.12.

Tables B.2.12.1 and B.2.12.2 provide the formats for pricing these services. CLINs fall under the following categories:

- Site Survey (includes site surveys for Special Access Construction, see Section B.2.9)
- Wiring Install

- Wiring Repair

Fixed price and ICB CLINs are specified for the categories listed above. Fixed prices represent typical cable and wiring activities as described in the Notes column of the Instructions Table B.2.12.2 below. All fixed-price CLINs include labor, travel, and material costs in the price. (e.g., connectors, faceplates, cable). If the fixed-price CLINs do not meet cable and wiring requirements, an ICB CLIN shall be used.

For each Wiring Install that is priced as ICB, the contractor must perform a Site Survey and provide a Site Survey Estimate with TO proposals or as specified in each TO by the customer. The estimate must include sufficient information to establish that the wiring install price is fair and reasonable. Section J.9 includes a Site Survey Estimate Template for Wiring Installs that identifies the type of data required.

B.2.12.1 Cable and Wiring Prices Table

CLIN	Case Number*	Task Order Number	Country / Jurisdiction ID**	Price	Price Start Date	Price Stop Date

* Applies only to ICB CLINs
** Country/Jurisdiction IDs are provided in Table B.4.2.1

B.2.12.2 Cable and Wiring Pricing Instructions Table

NRC CLIN	Description	Charging Unit	Notes
CW00001	Fixed Price Site Survey Basic ~~CONUS~~	Each	A site survey that does not require a site visit. The results are provided in a summary template. CONUS and OCONUS only.
CW00002	Fixed Price Site Survey Complex ~~CONUS~~	Each	A site survey requiring a site visit. The results are provided in a written quote, with documentation photos and drawings, as required. CONUS and OCONUS only.
~~CW00003~~	~~Fixed Price Site Survey Basic OCONUS~~	~~Each~~	~~A site survey that does not require a site visit. The results are provided in a summary template.~~
~~CW00004~~	~~Fixed Price Site Survey Complex OCONUS~~	~~Each~~	~~A site survey requiring a site visit. The results are provided in a written quote, with documentation photos and drawings, as required.~~
CW00005	ICB Site Survey	ICB	ICB. A site survey that cannot be accomplished under the Fixed Price Site Survey types. Examples include, but are not limited to, remote locations and extraordinary construction.

NRC CLIN	Description	Charging Unit	Notes
CW00101	Fixed Price Wiring Install ~~CONUS~~	Each	A wiring installation that can be accomplished on the customer's premises in 3 hours or less and includes up to 150 feet of wiring. The charges for the installation apply only when it is not coincident with an SRE installation. Price includes termination, jacks, and testing. CONUS and OCONUS only.
~~CW00102~~	~~Fixed Price Wiring Install OCONUS~~	~~Each~~	~~A wiring installation that can be accomplished on the customer's OCONUS premises in 3 hours or less and includes up to 150 feet of wiring. The charges for installation apply only when it does not coincide with an SRE installation. Price includes termination, jacks, and testing.~~
CW00103	ICB Wiring Install	ICB	ICB
CW00301	Fixed Price Wiring Repair ~~CONUS~~	Each	Restore inside wire service by dispatching qualified personnel to resolve a problem within 4 hours on site. CONUS and OCONUS only.
~~CW00302~~	~~Fixed Price Wiring Repair OCONUS~~	~~Each~~	~~Restore inside wire service by dispatching qualified personnel to resolve a problem within 4 hours on site.~~
CW00303	ICB Wiring Repair	ICB	ICB

B.3 National Security and Emergency Preparedness

The technical requirements for National Security and Emergency Preparedness (NS/EP) are defined in Sections C.1.8.8 and G.11.

B.3.1 NS/EP Price Structure

The price structure for the Telecommunications Service Priority (TSP) system of NS/EP includes the following elements:

1. NRC per circuit to register for priority installation, priority restorations, and priority level for design changes
2. MRC per circuit to maintain priority restorations

B.3.2 NS/EP Basic Prices

Table B.3.2.1 provides the formats for pricing information for TSP of NS/EP. Table B.3.2.2 provides the applicable charging mechanism and charging units for TSP of NS/EP.

B.3.2.1 NS/EP Prices Table

CLIN	Task Order Number	Price	Price Start Date	Price Stop Date

B.3.2.2 NS/EP Pricing Instructions Table

MRC CLIN	NRC CLIN	Description	Charging Unit
	NS00101	TSP Provisioning – No Local Access Coordination	Circuit
	NS00102	TSP Provisioning – One Local Access Coordination	Circuit
	NS00103	TSP Provisioning – Additional Local Access Coordination	Circuit
NS00004	NS00104	TSP Restorations – No Local Access Coordination	Circuit
NS00005	NS00105	TSP Restorations – One Local Access Coordination	Circuit
NS00006	NS00106	TSP Restorations – Additional Local Access Coordination	Circuit
	NS00107	TSP Priority Level for Design Change – No Local Access Coordination	Circuit
	NS00108	TSP Priority Level for Design Change – Local Access Coordination	Circuit

B.4 General Pricing and Other Requirements

This section defines pricing and other elements that are generally independent of the service categories. It also contains the requirements for contractor-provided domestic and non-domestic Point of Presence (POP) lists, Physical Concentration Locations (PCLs), Pricing Hubs (PHubs) and their service relationships. In addition, this section contains government-provided lists of Country/Jurisdiction IDs.

B.4.1 Point of Presence Identification, Location, and Service Relationships

EIS includes the following identifiers for infrastructure and pricing purposes:

- Network Site Code (NSC) – identifies a physical location, a customer agency building, Physical Concentration Location, and/or Point of Presence. An address is required for each NSC. GSA and EIS contractors will maintain an NSC database to ensure that every government location is associated with a single NSC identifier even where multiple addresses may refer to the same location. This allows services delivered to the government to be priced for each specific location using a unique NSC identifier represented by eight-character Common Language Location Identifier (CLLI) codes.
- Physical Concentration Location (PCL) – any place connections (e.g., copper wire, fiber and coax) are aggregated (e.g., POPs, carrier hotels, cable heads, and Serving Wire Centers (SWCs)). PCLs may refer to the access side of the service or to the network side. For pricing purposes, the PCL is identified by the NSC.
- Point of Presence (POP) – contractor-owned or -controlled physical location where network facilities provide EIS services and where access from a user agency's location is connected to the network. For pricing purposes, the POP is identified by the NSC.
- Pricing Hub (PHub) – used to assign a unique identifier to locations with the same price for the same access service type. This PHub ID is used only for pricing purposes and is independent of the physical network. The contractor selects and assigns a PHub ID to a set of prices by access type (i.e., by bandwidth).

Tables B.4.1.1 through B.4.1.11 provide the formats to list and identify domestic and non-domestic POPs, PCLs, PHubs, NSCs and their service relationships. Each POP shall be separately described by its physical location, as required by the individual table. The contractor shall keep these tables up to date as POPs, PCLs, PHubs, NSCs, and service relationships are added, deleted, and changed.

B.4.1.1 Domestic Points of Presence Table

POP NSC*	POP V&H Coordinates		Start Date	Stop Date
	V	H		

* POP NSCs shall be defined by the contractor in Table B.4.1.1 and are defined by the government in Table B.4.1.8

B.4.1.2 Non-Domestic Points of Presence Table

Country/ Jurisdiction ID in which POP is Located*	Non-Domestic POP NSC**	Name of Carrier or Entity Operating Non-Domestic POP, if not the Contractor	Start Date	Stop Date

* For country/jurisdiction names and IDs, see Table B.4.2.1
** Non-Domestic POP NSCs shall be defined by the contractor in Table B.4.1.2 and are defined by the government in Table B.4.1.8

Table B.4.1.3 provides the relationship between non-domestic sites and non-domestic POPs.

B.4.1.3 Non-Domestic Site to Point of Presence Relationship Table

Non-Domestic NSC	Non-Domestic POP NSC	Bandwidth Group*	Start Date	Stop Date

* Bandwidth Groups shall use the values in Table B.4.1.5.1

Table B.4.1.4 provides a list of services offered at each POP.

B.4.1.4 Services Offered by Point of Presence Table

POP NSC*	Service ID**	Bandwidth Group***	Start Date	Stop Date

* POP NSCs shall be defined by the contractor in Tables B.4.1.1 and B.4.1.2, and are defined by the government in Table B.4.1.8
** The contractor shall use this column to identify the services offered at each POP, to be selected from the following: VPNS, ETS, OWS, PLS, SONETS, DFS, IPS, CSVS, IPVS, CSDS, TFS, and MTIPS
*** Bandwidth Groups shall use the values in Table B.4.1.5.1

Table B.4.1.5 shall be populated, updated and maintained by the contractor to identify the PCL to POP relationship by bandwidth capability. The PCL serves as an engineering construct for purposes of identifying physical attributes of a networking solution, such as access routes needed to assure path diversity. At least one POP NSC shall be associated with each PCL NSC identified in Table B.4.1.5.

B.4.1.5 Domestic Physical Concentration Location to Point of Presence Relationship Table

PCL NSC*	Bandwidth Group**	POP NSC***

* PCLs are defined in Table B.4.1.8.
** Bandwidth Group shall use the values in Table B.4.1.5.1 Bandwidth Groups
*** POP NSCs shall be defined by the contractor in Tables B.4.1.1 and B.4.1.2, and are defined by the government in Table B.4.1.8

B.4.1.5.1 Bandwidth Groups Table

Bandwidth Group	Bandwidth Group Name	Minimum Bandwidth (Mbps)	Maximum Bandwidth (Mbps)
1	Wireline <=T1	0	1.54
2	Wireline >T1 and <=T3	1.55	44.74
3	Wireline >T3 and <=OC3	44.75	155.52
4	Wireline >OC3 and <=OC12	155.53	622.08
5	Wireline >OC12 and <=OC48	622.09	2,488.32
6	Wireline >OC48 and <=OC192	2,488.33	9953.28
7	Wireline >OC192 and <=OC768	9953.29	40,000.00
8	Ethernet <=10 Mbps	0	10.00
9	Ethernet >10 Mbps and <=100 Mbps	11.00	100.00
10	Ethernet >100 Mbps and <=1000 Mbps	101.00	1,000.00
11	Ethernet >1000 Mbps and <=10 Gbps	1,001.00	10,000.00
12	Ethernet >10 Gbps and <=100 Gbps	10,001.00	100,000.00
13	Ethernet >100 Gbps and <=1000 Gbps	100,001.00	1,000,000.00
14	Cable		
15	Dark Fiber		
16	Wireline >OC768	40,000.01	
17	Ethernet >1000 Gbps	1,000,001.00	

To identify multiple Bandwidth Groups for a PCL to POP relationship, the contractor shall populate the row with an array containing the applicable Group IDs. Arrays are denoted by a comma-separated list, surrounded by brackets, "{ }".

Table B.4.1.5.1.1 provides an example where PCL 1 has a relationship with POP A for every bandwidth group. Similarly, PCL 2 has a relationship with POP B for two bandwidth groups, and PCL 3 has a relationship with POP C for a single bandwidth group.

B.4.1.5.1.1 Example Bandwidth Group IDs for PCL to POP Relationship Table

PCL NSC	Bandwidth Group ID	POP NSC
1	{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15}	A
2	{8,12}	B
3	{9}	C

Table B.4.1.6 provides the relationship between Building NSCs and PCL NSCs.

The contractor may add sites after award at its option. As orders are submitted, new Building NSCs may need to be created for the locations involved. The contractor shall use iconectiv to obtain NSCs to represent any government building that orders service from an EIS contractor. The contractor shall interface with and use the iconectiv CLONES system to obtain and maintain NSC data. As new NSCs are created, the contractor shall use GSA Systems to update Tables B.4.1.6 and B.4.1.7 as needed to facilitate the validation of orders and invoices. Any order or invoice containing a building NSC that is not found in Tables B.4.1.6 and B.4.1.7 will be placed in dispute.

B.4.1.6 Network Site Code PCL Relationship Table

Building NSC*	PCL NSC*	Last Modified Date

* NSCs are defined in Table B.4.1.8

The contractor shall populate and maintain the relationship between Building NSCs and their respective PHubs in Table B.4.1.7. The PHubs in Table B.4.1.7 shall be used in conjunction with the access pricing tables in Section B.2.9 to set access prices. The government will reference Table B.4.1.6 to verify that the relationships within Table B.4.1.7 result in fair and reasonable prices as identified in the tables in Section B.2.9.

B.4.1.7 Network Site Code to Pricing Hub Relationship Table

Building NSC*	PHub ID	Access Type**	Last Modified Date

* NSCs are defined in Table B.4.1.8

** Indicate the Access Type as (1) Wireline, (2) Ethernet, (3) Cable, (4) FTTP, or (5) Wireless for the Building NSC-to-PHub relationship

The following reference tables will be updated and maintained by the government, and made available to the contractor, to validate all NSCs and NSC-to-PCL mappings maintained by the contractor. Tables B.4.1.8 and B.4.1.9 provide a list of domestic and non-domestic NSCs (these may be PCLs, SWCs, or government-identified buildings) and the associated location data.

B.4.1.8 Network Site Codes Table

NSC	Country/ Jurisdiction ID	Normalized Geographical Name	Latitude	Longitude	NSC V&H Coordinates		Created Date	Last Modified Date
					V	H		

B.4.1.9 Network Site Code/Address Correspondence Table

NSC	Sequence Number	Address						Address Intersection						Postal Code	County Name	Geo-political Code	Offset		Second Offset		Created Date	Last Modified Date
		Number	Prefix	Street Name	Street Type	Suffix	Unformatted Address	Option	Number	Prefix	Street Name	Street Type	Suffix				Distance	Direction	Distance	Direction		

Tables B.4.1.10 and B.4.1.11 identify PLS gateways and their relationships to non-domestic connections. The only valid relationships for Table B.4.1.11 are: 1) CONUS to OCONUS, 2) CONUS to Non-Domestic, and 3) OCONUS to Non-Domestic.

B.4.1.10 Domestic Private Line Service Gateways Table

Gateway ID	Gateway V&H Coordinates		Physical Address of Gateway				Start Date	Stop Date
	V	H	City	State	Street	Zip		

B.4.1.11 Domestic Private Line Service Gateway to OCONUS/Non-Domestic Country/Jurisdiction Relationship Table

Domestic Country/ Jurisdiction ID*	OCONUS/Non-Domestic Country Jurisdiction ID*	Gateway ID**	Start Date	Stop Date

* See Table B.4.2.1
** Defined in Section B.4.1.10

B.4.1.12 Metro OWS Locations

The contractor shall provide and maintain up-to-date locations where Metro OWS is being provided. Table B.4.1.12.1 provides the NSCs for those locations.

B.4.1.12.1 Metro OWS Locations Table

NSC

B.4.1.13 Order Related Prices

Table B.4.1.13.1 provides the pricing format for order related charges. Table B.4.1.13.2 provides the applicable charging mechanisms and charging units. Order requirements are described in Section G.3.3.2. Agencies may request order cancellations prior to issuance of the SOCN. Order cancellation charges shall not exceed the NRC of the cancelled order.

B.4.1.13.1 Order Related Prices

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.4.1.13.2 Order Charge Pricing Instructions

NRC CLIN	Description	Charging Unit	Notes
GN00001	Order Cancellation Charge	ICB	ICB

B.4.1.14 General Task Order Unique CLINs

Table B.4.1.14.1 provides the format for pricing TUCs for operational or administrative items (e.g., customized ordering, inventory or billing requirements, administrative customization) that are not readily associated with only one of the services defined in Table B.1.2.1.1. General TUCs shall not be used to price new services that are not listed in Table B.1.2.1.1. General TUCs shall be associated with and ancillary to the services in Table B.1.2.1.1, shall not be the primary purpose of a task order, and may only be ordered in conjunction with or in support of the purchase of services in Table B.1.2.1.1. Contractors may be required to provide additional information to support a determination that their proposed ancillary services are offered in support of one or more EIS CLINs. Table B.4.1.14.2 provides pricing instructions. TUCs shall be used as defined in Section B.1.2.15.

B.4.1.14.1 General TUC Prices Table

CLIN	Case Number	Task Order Number	Price	Price Start Date	Price Stop Date

B.4.1.14.2 General TUC Pricing Instructions Table

NRC CLIN	MRC CLIN	Usage CLIN	Description	Charging Unit	Notes
GN99990	GN99991	GN99992	General Task Order Unique	ICB	ICB

B.4.2 Country/Jurisdiction Identifications

Table B.4.2.1 provides Country/Jurisdiction IDs and Area of the World (AOW) IDs. The Country/Jurisdiction IDs shall be used in pricing tables that require identification of the origination and/or destination country/jurisdiction. The AOW IDs shall be used in pricing tables that allow for adjustments based on their OCONUS and Non-Domestic locations. For Wireless Service (MWS), Domestic is defined as CONUS, Alaska, Hawaii, Puerto Rico, and the U.S. Virgin Islands (see Section B.2.6).

B.4.2.1 Country/Jurisdiction Identification Table

Country/Jurisdiction	Country/ Jurisdiction ID*	AOW ID**	Location Type
Afghanistan	120038	200009	NONDOM
Albania	120039	200005	NONDOM
Algeria	120040	200011	NONDOM

Country/Jurisdiction	Country/ Jurisdiction ID*	AOW ID**	Location Type
Andorra	120042	200005	NONDOM
Angola	120043	200012	NONDOM
Anguilla	120044	200004	NONDOM
Antarctica	120045	200013	NONDOM
Antigua (includes Barbuda)	120046	200004	NONDOM
Argentina	120047	200004	NONDOM
Armenia	120048	200007	NONDOM
Aruba	120049	200004	NONDOM
Ascension Island	120050	200014	NONDOM
Australia	120051	200010	NONDOM
Australian External Territory	120309	200014	NONDOM
Austria	120052	200005	NONDOM
Azerbaijan	120053	200007	NONDOM
Azores	120300	200014	NONDOM
Bahamas	120054	200004	NONDOM
Bahrain	120055	200006	NONDOM
Bangladesh	120056	200009	NONDOM
Barbados	120057	200004	NONDOM
Belarus	120058	200005	NONDOM
Belgium	120059	200005	NONDOM
Belize	120060	200004	NONDOM
Benin	120061	200012	NONDOM
Bermuda	120062	200003	NONDOM
Bhutan	120063	200009	NONDOM
Bolivia	120064	200004	NONDOM
Bosnia - Herzegovina	120065	200005	NONDOM
Botswana	120066	200012	NONDOM
Brazil	120067	200004	NONDOM
British Indian Ocean Territories	120313	200014	NONDOM
British Virgin Islands	120068	200004	NONDOM
Brunei	120069	200012	NONDOM
Bulgaria	120070	200005	NONDOM
Burkina Faso	120071	200012	NONDOM
Burundi	120073	200012	NONDOM
Cambodia	120074	200009	NONDOM
Cameroon	120075	200012	NONDOM
Canada	120076	200003	NONDOM
Cape Verde Islands	120077	200014	NONDOM

Country/Jurisdiction	Country/ Jurisdiction ID*	AOW ID**	Location Type
Cayman Islands	120078	200004	NONDOM
Central African Republic	120079	200012	NONDOM
Chad	120080	200012	NONDOM
Chatham Island	120302	200014	NONDOM
Chile	120081	200004	NONDOM
China	120082	200009	NONDOM
Christmas Island	120083	200014	NONDOM
Cocos Islands	120084	200014	NONDOM
Colombia	120085	200004	NONDOM
Comoros	120086	200014	NONDOM
Congo, Dem. Republic Of The	120266	200012	NONDOM
Congo, Republic Of The	120087	200012	NONDOM
Cook Islands	120088	200014	NONDOM
Costa Rica	120089	200004	NONDOM
Cote d'Ivoire	120143	200012	NONDOM
Croatia	120090	200005	NONDOM
Cuba	120091	200004	NONDOM
Cyprus - North	120303	200006	NONDOM
Cyprus - South	120304	200005	NONDOM
Czech Republic	120093	200005	NONDOM
Denmark	120094	200005	NONDOM
Diego Garcia	120095	200014	NONDOM
Djibouti	120096	200012	NONDOM
Domestic: Alaska	120036	200001	OCONUS
Domestic: American Samoa***	179627	200002	OCONUS
Domestic: Commonwealth of Northern	120270	200002	OCONUS
Domestic: CONUS	120033	200000	CONUS
Domestic: Guam***	120269	200001	OCONUS
Domestic: Hawaii	120037	200001	OCONUS
Domestic: Marshall Islands***	120171	200002	OCONUS
Domestic: Micronesia***	120176	200002	OCONUS
Domestic: Midway Island***	120177	200002	OCONUS
Domestic: Palau***	120199	200002	OCONUS
Domestic: Puerto Rico	120316	200001	OCONUS
Domestic: US Virgin Islands (USVI)	120317	200001	OCONUS
Domestic: Wake Island***	120261	200002	OCONUS
Dominica	120097	200004	NONDOM
Dominican Republic	120098	200004	NONDOM

Country/Jurisdiction	Country/ Jurisdiction ID*	AOW ID**	Location Type
East Timor	120305	200009	NONDOM
Easter Island	120099	200014	NONDOM
Ecuador	120100	200004	NONDOM
Egypt	120101	200006	NONDOM
El Salvador	120102	200004	NONDOM
Equatorial Guinea	120103	200012	NONDOM
Eritrea	120104	200012	NONDOM
Estonia	120105	200005	NONDOM
Ethiopia	120106	200012	NONDOM
Faeroe Islands	120107	200014	NONDOM
Falkland Islands	120108	200014	NONDOM
Fiji Islands	120109	200014	NONDOM
Finland	120110	200005	NONDOM
France	120111	200005	NONDOM
French Antilles	120112	200004	NONDOM
French Guiana	120113	200004	NONDOM
French Polynesia	120114	200014	NONDOM
French Southern Territory	120314	200014	NONDOM
Gabon	120115	200012	NONDOM
Gambia	120116	200012	NONDOM
Georgia	120117	200007	NONDOM
Germany	120118	200005	NONDOM
Ghana	120119	200012	NONDOM
Gibraltar	120120	200005	NONDOM
Global Sat	180025***	****	NONDOM
Greece	120121	200005	NONDOM
Greenland	120122	200014	NONDOM
Grenada	120123	200004	NONDOM
Guadeloupe	120124	200004	NONDOM
Guantanamo Bay	120126	200004	NONDOM
Guatemala	120127	200004	NONDOM
Guinea	120129	200012	NONDOM
Guinea - Bissau	120128	200012	NONDOM
Guyana	120130	200004	NONDOM
Haiti	120131	200004	NONDOM
Honduras	120132	200004	NONDOM
Hong Kong, Special Administrative District	120133	200009	NONDOM
Hungary	120134	200005	NONDOM

Country/Jurisdiction	Country/ Jurisdiction ID*	AOW ID**	Location Type
Iceland	120135	200005	NONDOM
India	120136	200009	NONDOM
Indonesia	120137	200009	NONDOM
Inmarsat Aero	180029***	****	NONDOM
Inmarsat Broadband Global Area Network	180041***	****	NONDOM
Inmarsat Broadband Global Area Network	180043***	****	NONDOM
Inmarsat Broadband Global Area Network	180042***	****	NONDOM
Inmarsat Fleet (Maritime) I4-Americas	180038***	****	NONDOM
Inmarsat Fleet (Maritime) I4-Asia Pacific	180040***	****	NONDOM
Inmarsat Fleet (Maritime) I4-EMEA (Europe,	180039***	****	NONDOM
Inmarsat Global Express (GX) I5-AOR	180047***	****	NONDOM
Inmarsat Global Express (GX) I5-IOR	180048***	****	NONDOM
Inmarsat Global Express (GX) I5-POR	180049***	****	NONDOM
Inmarsat Mini-M	180036***	****	NONDOM
Inmarsat Swift (Aeronautical) Atlantic (AOR)	180044***	****	NONDOM
Inmarsat Swift (Aeronautical) Indian (IOR)	180045***	****	NONDOM
Inmarsat Swift (Aeronautical) Pacific (POR)	180046***	****	NONDOM
Iran	120138	200006	NONDOM
Iraq	120139	200006	NONDOM
Ireland	120140	200005	NONDOM
Iridium-8816	180026***	****	NONDOM
Iridium-8817	180027***	****	NONDOM
Israel	120141	200006	NONDOM
Italy	120142	200005	NONDOM
Jamaica	120144	200004	NONDOM
Japan (includes Okinawa)	120145	200008	NONDOM
Jordan	120146	200006	NONDOM
Kazakhstan	120147	200007	NONDOM
Kenya	120148	200012	NONDOM
Kiribati	120149	200014	NONDOM
Kosovo	120306	200005	NONDOM
Kuwait	120152	200006	NONDOM
Kyrgyzstan	120153	200007	NONDOM
Laos	120154	200009	NONDOM
Latvia	120155	200005	NONDOM
Lebanon	120156	200006	NONDOM
Lesotho	120157	200012	NONDOM
Liberia	120158	200012	NONDOM

Country/Jurisdiction	Country/ Jurisdiction ID*	AOW ID**	Location Type
Libya	120159	200011	NONDOM
Liechtenstein	120160	200005	NONDOM
Lithuania	120161	200005	NONDOM
Luxembourg	120162	200005	NONDOM
Macau, Special Administrative District	120163	200009	NONDOM
Macedonia	120164	200005	NONDOM
Madagascar	120165	200012	NONDOM
Malawi	120166	200012	NONDOM
Malaysia	120167	200009	NONDOM
Maldives	120168	200014	NONDOM
Mali	120169	200012	NONDOM
Malta	120170	200005	NONDOM
Martinique	120310	200004	NONDOM
Mauritania	120172	200012	NONDOM
Mauritius	120173	200012	NONDOM
Mayotte Island	120174	200014	NONDOM
Mexico	180020	200003	NONDOM
Moldova	120178	200005	NONDOM
Monaco	120179	200005	NONDOM
Mongolia	120180	200009	NONDOM
Montenegro	120320	200005	NONDOM
Montserrat	120181	200004	NONDOM
Morocco	120182	200011	NONDOM
Mozambique	120183	200012	NONDOM
Myanmar	120072	200009	NONDOM
Namibia	120184	200012	NONDOM
Nauru	120185	200014	NONDOM
Nepal	120186	200009	NONDOM
Netherlands	120187	200005	NONDOM
Netherlands Antilles	120188	200004	NONDOM
Nevis	120032	200004	NONDOM
New Caledonia	120189	200014	NONDOM
New Zealand	120190	200010	NONDOM
Nicaragua	120191	200004	NONDOM
Niger	120192	200012	NONDOM
Nigeria	120193	200012	NONDOM
Niue	120194	200014	NONDOM
Norfolk Island	120195	200014	NONDOM

Country/Jurisdiction	Country/ Jurisdiction ID*	AOW ID**	Location Type
North Korea	120150	200009	NONDOM
Norway (includes Svalbard)	120196	200005	NONDOM
Oman	120197	200006	NONDOM
Pakistan	120198	200009	NONDOM
Palestinian Authority	120307	200006	NONDOM
Panama	120200	200004	NONDOM
Papua New Guinea	120201	200009	NONDOM
Paraguay	120202	200004	NONDOM
Peru	120203	200004	NONDOM
Philippines	120204	200008	NONDOM
Pitcairn Island	120205	200014	NONDOM
Poland	120206	200005	NONDOM
Portugal (includes Madeira)	120207	200005	NONDOM
Qatar	120208	200006	NONDOM
Reunion Island	120209	200014	NONDOM
Romania	120210	200005	NONDOM
Russia	120211	200007	NONDOM
Rwanda	120212	200012	NONDOM
Samoa	120264	200014	NONDOM
San Marino	120219	200005	NONDOM
Sao Tome	120220	200012	NONDOM
Saudi Arabia	120221	200006	NONDOM
Senegal	120222	200012	NONDOM
Serbia	120223	200005	NONDOM
Seychelles Islands	120224	200012	NONDOM
Sierra Leone	120225	200012	NONDOM
Singapore	120226	200009	NONDOM
Slovakia	120227	200005	NONDOM
Slovenia	120228	200005	NONDOM
Solomon Islands	120229	200014	NONDOM
Somalia	120230	200012	NONDOM
South Africa	120231	200012	NONDOM
South Korea	120151	200008	NONDOM
South Sudan	120272	200012	NONDOM
Spain (includes Balearic Islands, Canary	120232	200005	NONDOM
Sri Lanka	120233	200009	NONDOM
St. Helena	120213	200014	NONDOM
St. Kitts	120214	200004	NONDOM

Country/Jurisdiction	Country/ Jurisdiction ID*	AOW ID**	Location Type
St. Lucia	120215	200004	NONDOM
St. Pierre And Miquelon	120216	200003	NONDOM
St. Vincent And The Grenadines	120217	200004	NONDOM
Sudan	120234	200012	NONDOM
Suriname	120235	200004	NONDOM
Swaziland	120236	200012	NONDOM
Sweden	120237	200005	NONDOM
Switzerland	120238	200005	NONDOM
Syria	120239	200006	NONDOM
Taiwan	120240	200008	NONDOM
Tajikistan	120241	200007	NONDOM
Tanzania	120242	200012	NONDOM
Thailand	120243	200009	NONDOM
Thuraya Sat	180037***	****	NONDOM
Togo	120244	200012	NONDOM
Tokelau	120308	200014	NONDOM
Tonga Islands	120245	200014	NONDOM
Trinidad And Tobago	120246	200004	NONDOM
Tunisia	120247	200011	NONDOM
Turkey	120248	200006	NONDOM
Turkmenistan	120249	200007	NONDOM
Turks And Caicos Islands	120250	200004	NONDOM
Tuvalu	120251	200014	NONDOM
Uganda	120252	200012	NONDOM
Ukraine	120253	200005	NONDOM
United Arab Emirates	120254	200006	NONDOM
United Kingdom	120255	200005	NONDOM
Uruguay	120256	200004	NONDOM
Uzbekistan	120257	200007	NONDOM
Vanuatu	120258	200014	NONDOM
Vatican City	120312	200005	NONDOM
Venezuela	120259	200004	NONDOM
Vietnam	120260	200009	NONDOM
Wallis And Futuna Islands	120262	200014	NONDOM
Western Sahara	120263	200014	NONDOM
Yemen	120265	200006	NONDOM
Zambia	120267	200012	NONDOM
Zanzibar (Province Of Tanzania)	120318	200012	NONDOM

Country/Jurisdiction	Country/ Jurisdiction ID*	AOW ID**	Location Type
Zimbabwe	120268	200012	NONDOM

***** IDs shall be fixed through the life of the contract unless changed by contract modification.
** The AOW ID applicable to mobile SRE is the location at which it is installed, if vehicle mounted, or the location from which it is shipped, if it is designed to be carried on the person.

******* Excluded from domestic Wireless Service (Section B.2.6).
**** Satellite IDs.

Enterprise Infrastructure Solutions (EIS)
Contract

Section C
Description / Specifications / Statement of Work

Issued by:

General Services Administration

Office of Integrated Technology Services

[redacted]

~~FEBRUARY~~May 2018

Table of Contents

C.1 Background

The General Services Administration (GSA), Federal Acquisition Service, Integrated Technology Services (ITS), Network Services Program (NSP[1]) establishes and manages a range of acquisition programs to meet the needs of federal agencies for telecommunications, networking services and associated support.

This Request for Proposals (RFP) describes the government's requirements for the Enterprise Infrastructure Solutions (EIS) contract.

C.1.1 EIS Goals

The EIS contract is intended to meet the program goals for:

- Service Continuity.
- Highly Competitive Prices.
- High-Quality Service.
- Full Service Vendors.
- Operations Support.
- Transition Assistance and Support.

The overarching goal for EIS is to make the resulting contracts as flexible and agile as possible to meet and satisfy the widely differing requirements of the federal agencies both now and for the next decade and beyond.

C.1.2 EIS Scope for Mandatory and Optional Services

The EIS mandatory services include the following:

- Virtual Private Network Service — Specified in Section C.2.1.1
- Ethernet Transport Service — Specified in Section C.2.1.2
- Voice — Specified in Section C.2.2.1 and C.2.2.2
- Managed Network Service — Specified in Section C.2.8.1

It should be noted that Access Arrangements (Section C.2.9) are included as a mandatory component and shall be priced. The contractor shall also provide Voice services to non-domestic locations as defined in Section J.1.2.

Any service included in Section C.1.8.1 that is not listed above is considered optional.

[1] See http://www.gsa.gov/portal/category/22151 for background

C.1.3 Minimum Requirements for Geographic Coverage

The contractor shall provide EIS services on a global basis. Geographic coverage for domestic and non-domestic locations is specified in Section J.1. Domestic locations are further divided into CONUS and OCONUS.

CONUS Geographic requirements are defined by a set of domestic cities, based on the Core Based Statistical Areas (CBSAs) as defined in OMB Bulletin No. 13-01, dated February 28, 2013. The minimum mandatory geographic coverage area includes any 25 of the top 100 CBSAs provided by the government in Section J.1. The CBSAs listed are ranked in descending order of government bandwidth usage. It should be noted that there are over 900 CBSAs in the U.S. requiring services.

Notwithstanding the minimum requirements, the contractor is encouraged to propose the mandatory and optional services within any CBSA, OCONUS or non-domestic locations, whether included in Section J.1 or not, as long as the offer includes at least 25 of the top 100 CBSAs listed in Section J.1.

The contractor shall provide the mandatory services to all government locations within each of its selected CBSAs.

C.1.4 Task Orders

The government will order services in accordance with FAR Subpart 16.505. Agencies will conduct fair opportunity and award task orders (TOs) in accordance with the aforementioned subpart and the terms and conditions of this contract. For more detail, see Section G.3.

C.1.5 Authorized Users

This contract is for the use of all federal agencies, authorized federal contractors, agency-sponsored universities and laboratories, other organizations as defined in Section H.3, and, when authorized by law or regulation, state, local, and tribal governments.

C.1.6 Upgrades and Enhancements

The government recognizes that telecommunications technologies and services are rapidly evolving. Accordingly, the government anticipates that services and solutions available under this contract will be increased, enhanced, and upgraded as these improvements become available to commercial customers.

As the virtualization of infrastructure continues from computing to networking, the government is interested in the deployment roll-out of Network Function Virtualization

and Software Defined Network (NFV/SDN) in the contractor's backbone wide area network (WAN), because the SDN supports quick provisioning and easy management.

Network function virtualization (NFV) is the virtualization of network equipment functions, which typically run on dedicated appliances, to now run on industry-standard servers, switches and storage devices with the aim of lowering costs, improving efficiency and increasing agility, via hypervisor technologies. Standards are being created by the European Telecommunications Standards Institute (ETSI), including major telecom equipment vendors and communications service providers (CSPs), with involvement by the Open Networking Foundation.

Software Defined Networking (SDN) is an approach to networking in which control is decoupled from the physical infrastructure, allowing network administrators to support a network fabric across multi-vendor equipment. The SDN decouples network control and forwarding functions, enabling network control to become directly programmable and the underlying infrastructure to be abstracted from applications and network services, by supporting the following capabilities:

1. Transport independence by disaggregating the service from the physical network.
2. Security (encryption and device authentication) at the routing level.
3. Allow network segmentation with different segments having different encryption schemes.
4. Centralized policy and control of all the devices across the network.
5. Allow Layer 4-7 services (to be advertised) on demand.

This will allow network managers, both agency and service providers, to configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs/codes (APIs), which they can write themselves because the programs/codes do not depend on proprietary software.

C.1.7 Organization of this Statement of Work

Section C.2 provides the technical requirements addressed by this contract. Section C.1.8 describes the general requirements and the format for the specification of the individual service areas and services, which are contained in Sections C.2.1 through C.2.12. Section C.3 contains requirements for management of transition from another expiring GSA-administered contract to EIS. Section C.4 specifies the government's requirements for Section 508 compliance that have been established to ensure access to information and services by government employees and citizens with disabilities.

C.1.8 General Requirements

C.1.8.1 Organization of EIS Services

EIS service areas and services are presented in the following table.

Service Area	Service
Data Service	VPNS Ethernet Transport Optical Wavelength Service Private Line SONET Dark Fiber Internet Protocol Service
Voice Service	IP Voice Service Circuit Switched Voice Service Toll Free Service CSDS
Contact Center Service	Contact Center Service
Colocated Hosting Service	Data Center Service
Cloud Service	Infrastructure as a Service Platform as a Service Software as a Service Content Delivery Network Service
Wireless Service	Wireless Service
Commercial Satellite Service	Satellite Service

Service Area	Service
Managed Services	Managed Network Service Web Conferencing Service Unified Communications Service Managed Trusted Internet Protocol Service Managed Security Service Managed Mobility Service Audio conferencing Video Teleconferencing Intrusion Prevention Security Service
Access Arrangements	Access Arrangements
Service Related Equipment	Equipment
Service Related Labor	Labor
Cable and Wiring	Cable and Wiring

IT-related products and services listed in the table above may be acquired only if they are associated to an infrastructure or telecommunications solution acquired through EIS.

C.1.8.2 Service Locations

A Service Delivery Point (SDP) is the interface point at which a service is delivered by the contractor to the government or its designated agent. The SDP is the interface point for the physical or logical delivery of a service and the point at which performance parameters are measured to determine compliance with the contract.

C.1.8.3 Performance

Almost all EIS services have a specified standard set of common metrics or Key Performance Indicators (KPIs) to measure and report their performance. This standard set of KPI's measures the primary dimensions an agency needs in order to evaluate service effectiveness. The underlying KPI computations are service specific or context sensitive (as defined within each service) to reflect the broad range of service offerings and the EIS focus on delivery of end to end services. The seven standard KPIs used for most services as specified within this contract are defined below.

Standard KPIs:

No.	KPI	Abbreviation
1	Availability (Service)	Av(S)
2	Time to Restore	TTR
3	Grade of Service (Service)	GOS(S)
4	Latency (Service)	Latency(S)
5	Jitter	Jitter
6	Event Notification	EN
7	Response Time	RT

For certain services, when required by agency customers, two service levels are specified. Routine service levels apply for most government applications. Critical service levels are defined for agency applications requiring higher levels of availability, performance, or restoral criteria. Critical service levels will be sought in the TO fair opportunity process. The parameters specified in the service descriptions shall apply to all domestic (both CONUS and OCONUS) services. Performance parameters for non-domestic services are specified in Section C.1.8.5. In addition, the performance provided shall always be at a level not less than what is generally available commercially, at no additional cost to the government. Thus, if the available commercial performance parameter is more demanding than the minimum acceptable level specified in this contract, the available commercial performance parameter shall take precedence.

As standards evolve, the contractor may propose and provide alternatives to the government that meet or exceed the standards listed per specific service.

C.1.8.4 Conformity to Standards

Throughout Section C, references are made to standards (including interim standards, Internet Engineering Task Force (IETF) Requests for Comments (RFCs), or de-facto standards) as they existed at the time of contract award. If a standard is defined by a specific version and/or date, then that specific version of the standard shall be implemented. Otherwise, compliance with the latest versions of these standards is expected. American national standards shall supersede international standards for services to be provided to on-net users located in the U.S. Where multiple standards

are cited, the order of precedence shall be the industry forum specification, followed by ANSI, followed by iconectiv, and followed by ITU-TSS, unless otherwise specified.

C.1.8.5 Non-Domestic

Coverage includes delivery of service from domestic SDPs to non-domestic SDPs, from non-domestic SDPs to domestic SDPs, and from non-domestic SDPs to non-domestic SDPs. The following requirements for the numbering plan, features, performance, interfaces, security, and management and operations considerations that are applicable to the non-domestic services shall supersede the corresponding requirements specified for the domestic services:

1. **Numbering Plan.** The numbering plan for non-domestic locations shall conform to country-specific numbering plans.
2. **Features.** All features identified as mandatory in each service description shall be provided to non-domestic SDPs in the areas involved.
3. **Dial-In.** The contractor shall support country-specific non-domestic PSTN numbers and/or toll-free numbers, if commercially available, for dial-in access of services.
4. **Performance.** The KPIs in the performance metrics for each service between non-domestic SDPs or between domestic and non-domestic SDPs shall be compliant with the best commercial values or practices for those parameters within the non-domestic country and/or jurisdiction hosting the non-domestic SDPs.
5. **Interfaces.** When a service is delivered to an SDP at a non-domestic location, the UNI, e.g., interface type, payload data rate, protocol type, standard for the SDP shall comply with the country-specific interface standards when delivering service to the country-specific government equipment. However, if the government equipment conforms to a North American standard, then the UNI standard at the SDP shall comply with the North American standard where permitted by local law and regulations.

C.1.8.6 Interoperability

The contractor shall support interoperability for given service offerings so that a user of a service from one EIS contractor shall be able to communicate with users of services from other EIS contractors with equivalent performance. GSA recognizes that different levels of interoperability exist commercially, particularly in the area of data networking. Interoperability shall be made available for any service that is currently commercially offered by the contractor and is interoperable with the services of other EIS contractors.

In addition, the contractor shall make available any future service interoperability at no additional cost to GSA when the contractor offers the interoperability for its commercially provided service.

Since near full interoperability is provided via the Public Switched Telephone Network (PSTN) for circuit switched services, the contractor shall support interoperability between voice services, circuit switched data service, and wireless services if offered. The contractor shall also support connectivity and interoperability for remote and mobile users as specified in the individual service descriptions.

C.1.8.7 System Security Requirements

Communications services under this contract will carry non-sensitive programmatic and administrative traffic, Controlled Unclassified Information (CUI) traffic, and higher levels of sensitive and/or classified traffic up to and including Top Secret/SCI that may be encrypted by agency users. Therefore, the contractor is required to provide basic security for all network services, as well as the network management systems and information systems and databases used to support those services. Such security shall include protecting all network services, information, contractor infrastructure, and information processing resources against threats, attacks, or failures of systems.

The contractor shall ensure that all services provided comply with all Federal Information Security Management Act (FISMA), DOD, and Intelligence Community requirements where applicable. The contractor shall submit a Risk Management Framework Plan describing its approach for security compliance for all services provided under EIS. This plan shall be submitted with the proposal in accordance with National Institute of Standards (NIST) Special Publication (SP) 800-37.

C.1.8.7.1 System Security Compliance Requirements

In providing EIS services, the contractor shall comply with all applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements. The contractor shall comply with FISMA, DOD and Intelligence Community-associated guidance and directives to include all applicable Federal Information Processing Standards (FIPS), NIST SP 800 series guidelines (FIPS and NIST SPs available at: http://csrc.nist.gov/), agency-specific security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of government IT. In addition, the contractor shall comply with all service specific security requirements identified within Section C.2 Technical Requirements (e.g., Cloud Infrastructure as a Service (IaaS), or Managed Trusted Internet Protocol Services (MTIPS)).

Compliance references include, but are not limited to:

- Federal Information Security Management Act (FISMA) of 2002; (44 U.S.C. Section 301. Information security) available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
- Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.) available at https://www.congress.gov/113/bills/s2521/BILLS-113s2521es.pdf.
- Clinger-Cohen Act of 1996 (formerly known as the "Information Technology Management Reform Act of 1996") available at: https://www.fismacenter.com/Clinger%20Cohen.pdf.
- Privacy Act of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and contractors", dated August 27, 2004; available at: http://www.idmanagement.gov/.
- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources", and Appendix III, "Security of Federal Automated Information Systems", as amended; available at: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/.
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies" (Available at: http://www.whitehouse.gov/omb/memoranda_2004).
- OMB Memorandum M-14-03. "Enhancing the Security of Federal Information and Information Systems" available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems." Dated February 2004.
- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems." Dated March 2006.
- FIPS PUB 140-2, "Security Requirements for Cryptographic Modules." Dated May 2001.
- NIST SP 800-18 Revision 1, "Guide for Developing Security Plans for Federal Information Systems." Dated February 2006.
- NIST SP 800-30 Revision 1, "Guide for Conducting Risk Assessments." Dated September 2012.
- NIST SP 800-34 Revision 1, "Contingency Planning Guide for Information Technology Systems." Dated May 2010.
- NIST SP 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach." Dated February 2010.

- NIST SP 800-40 Revision 3, “Guide to Enterprise Patch Management Technologies.” Dated July 2013.
- NIST SP 800-41 Revision 1, “Guidelines on Firewalls and Firewall Policy.” Dated September 2009.
- NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems.” Dated August 2002.
- NIST Special Publication 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations.” Dated April 2013.
- NIST Special Publication 800-53A, Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans.” Dated December 2014.
- NIST SP 800-58 “Security Considerations for Voice Over IP Systems.” Dated January 2005.
- NIST SP 800-60 Revision 1, “Guide for Mapping Types of Information and Information Systems to Security Categories.” Dated August 2008.
- NIST SP 800-61 Revision 2, “Computer Security Incident Handling Guide.” Dated August 2012.
- NIST SP 800-88 Revision 1, “Guidelines for Media Sanitization.” Dated December 2014.
- NIST SP 800-94 “Guide to Intrusion Detection and Prevention Systems.” Dated February 2007.
- NIST SP 800-128 “Guide for Security-Focused Configuration Management of Information Systems.” Dated August 2011.
- NIST SP 800-137 “Information Security Continuous Monitoring for Federal Information Systems and Organizations.” Dated September 2011.
- NIST SP 800-144 “Guidelines on Security and Privacy in Public Cloud Computing.” Dated December 2011.
- NIST SP 800-160 “Systems Security Engineering.” dated November 2016.
- NIST SP 800-161 “Supply Chain Risk Management Practices for Federal Information Systems and Organizations.” Dated April 2015.
- NIST SP 800-171, “Protecting Controlled Unclassified Information in the Nonfederal Information Systems and Organizations.” Dated June 2015.
- Committee on National Security Systems (CNSS) Policy No. 12, National Information Assurance Policy for Space Systems Used to Support National Security Missions. Dated 28 November 2012.

- Committee on National Security Systems (CNSS) Policy No. 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems. Dated 1 October 2012.
- Committee on National Security Systems Instruction (CNSSI) No. 1253, Security Categorization and Control Selection for National Security Systems. Dated March 2012.
- Committee on National Security Systems Instruction (CNSSI) No. 5000, "Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony." Dated April 2007.
- Department of Defense Instruction (DODI) 8500.01 "Cybersecurity." Dated 14 March 2014.
- DODI 8510.01 "Risk Management Framework (RMF) for DOD Information Technology (IT)." Dated 12 March 2014.
- Department of Defense (DOD) Cloud Computing Security Requirements Guide (SRG). Draft Dated 7 December 2014.
- ICD 503, "Intelligence Community Information Technology Systems Security: Risk Management, Certification and Accreditation." Dated 15 September 2008.
- ICD 703, "Protection of Classified National Intelligence, Including Sensitive Compartmented Information." Dated 21 June 2013.
- ICD 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information." Dated 1 October 2008.
- ICD 705, "Sensitive Compartmented Information Facilities." Dated 26 May 2010.
- ICD 731, "Supply Chain Risk Management." Dated 7 December 2013.
- Other agency-specific policies, directives and standards as identified at the TO level.

C.1.8.7.2 Security Compliance Requirements

FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in eighteen security-related areas. Contractor systems supporting agencies must meet the minimum security requirements through the use of the security controls in accordance with NIST Special Publication 800-53, Revision 4 (hereinafter described as NIST SP 800-53) "Recommended Security Controls for Federal Information Systems."

To comply with the federal standard, the government has determined the security category of the information and information system in accordance with FIPS 199,

"Standards for Security Categorization of Federal Information and Information Systems," to be established at a minimum of a Moderate Impact Level and baseline security controls must be established as identified in NIST SP 800-53 and other associated directives and guides identified and/or provided by each specific agency.

The government recognizes that these requirements are evolving and will make the necessary updates as the standards are formally implemented to reflect the changes.

If a Cloud solution is used (meeting the NIST definition of Cloud as stated in C.2.5) the security category of the information and information system will be established at a minimum of a Moderate Impact Level and the baseline security controls, applicable directives and guides as well as deliverables that must be adhered to are identified at www.FedRAMP.gov.

GSA will not be an EIS contractor FedRAMP sponsor at the contract level.

C.1.8.7.3 Security Assessment and Authorization (Security A&A)

In addition to the contractor's Business Support System (BSS) requirements identified in Section G.5.6, the implementation of any contractor IT system that stores, transports or processes federal government data requires a formal approval process known as security A&A. NIST SP 800-37, Revision 1 (hereinafter listed as NIST SP 800-37) and agency-specific IT security procedural guidance, associated with managing enterprise risk, provides guidance for performing the security A&A process.

The contractor's system must have the capability to provide a valid security A&A (when required by agency TO) prior to being placed into operation and processing government information for that agency. Agencies may require higher level certifications to be addressed at the TO level. Failure to obtain and maintain a valid assessment and authorization will be grounds for termination of a TO.

C.1.8.7.4 System Security Plan (SSP)

For delivery of services under a TO, the contractor shall comply with all security A&A requirements mandated by federal laws, directives and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The level of effort for the security assessment and authorization is based on the System's NIST FIPS Publication 199 categorization. The SSP shall be completed in accordance with NIST Special Publication 800-18, Revision 1 (hereinafter listed as NIST SP 800-18) and other relevant guidelines. The SSP shall describe the contractor's approach for security compliance for all services provided under the EIS contract. The SSP shall also include, at a minimum, appendices and attachments specifically identified within the TO.

C.1.8.7.5 System Security Plan Deliverables

TOs will specifically identify the system security deliverables to be provided to an Ordering Contracting Officer (OCO), Information System Security Officer (ISSO), or Information System Security Manager (ISSM) initially, quarterly and on an annual basis, or when significant changes, as defined in NIST SP 800-37, occur to the system.

C.1.8.7.6 Additional Security Requirements

ID Number	Description
1	The deliverables identified in Section C.1.8.7.5 shall be labeled "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) or contractor selected designation per document sensitivity. External transmission/dissemination of CUI data to or from an agency computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "*Security requirements for Cryptographic Modules.*"
2	The government has the right to perform manual or automated audits, scans, reviews, or other inspections of the contractor's IT environment being used to provide or facilitate services for the government. In accordance with the FAR (see Section I, 52.239-1) the contractor shall be responsible for the following privacy and security safeguards: 1. The contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the contractor under this TO or otherwise provided by the government. *Exception - Disclosure to a Consumer Agency for purposes of security assessment and authorization verification.* 2. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, availability and confidentiality of any non-public government data collected and stored by the contractor, the contractor shall afford the government logical and physical access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods: • Authenticated and unauthenticated operating system/network vulnerability scans, • Authenticated and unauthenticated web application vulnerability scans, • Authenticated and unauthenticated database application vulnerability scans, and • Internal and external penetration tests. 3. Automated scans can be performed by government personnel, or agents acting on behalf of the government, using government operated equipment, and government specified tools. If the contractor chooses to run its own automated scans or audits, results from these scans may, at the government's discretion, be accepted in lieu of government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the government. In addition, the results of contractor-conducted scans shall be provided, in full, to the government.

C.1.8.7.7 Personnel Background Investigation Requirements

The contractor shall perform personnel security / suitability checking in accordance with FAR Part 52.204-9 (see Section I).

All contractor personnel with access to government information that is within the security A&A scope must successfully complete a background investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12) Office of Management and Budget (OMB) guidance M-05-24, M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors," and as specified in agency-identified security directives and procedural guides.

The ordering agency will be responsible for the cost of any required background investigations.

C.1.8.8 National Policy Requirements

The concept of a national telecommunications infrastructure is recognized in national policy statements and directives issued under the authority of the Executive Office of the President, Congress, the Department of Homeland Security (including the Office of Emergency Communications), and other entities of the government. This telecommunications infrastructure is required to support the critical needs of the government under conditions of stress that range from crises and natural disasters (e.g., flood, earthquake) through declared conditions of National Security and Emergency Preparedness (NS/EP). Public safety and the economic well-being of the nation also depend upon the availability of reliable and responsive telecommunications services. EIS is a key component of the US national telecommunications infrastructure.

GSA expects to effectively provide assurance for government users that services and service elements (technical, management and operations-related) acquired through EIS will be in compliance with national policy throughout the life of the contracts. The contractor shall ensure that services delivered are in compliance with national policy directives that apply to the national telecommunications infrastructure.

Specific national policy requirements include, but are not limited to:

1. NS/EP requirements include a wide range of Executive Orders, Presidential Directives as promulgated by the Executive Office of the President, the Director of Homeland Security, the Office of Emergency Communications and other government entities. NS/EP requirements are covered in Section G.11.
2. OMB Memorandum M-05-22 directs that agencies must transition from IPv4 agency infrastructures to IPv6 agency infrastructures (network backbones). For agencies with an IPv6 network (and those implementing IPv6 networks) with IPv4

legacy support, the contractor solution must maintain functionality and shall comply with NIST SP 500-267. All systems, software, and equipment supporting the agency network and its services shall handle IPv6 in an equivalent or better way than current IPv4 capabilities, performance, and security. No systems, software, or equipment shall be deployed on the network that does not meet this requirement. Additionally, all network management shall be enabled using IPv6.

3. OMB Memorandum M-09-32, "Update on the Trusted Internet Connections Initiative," "requires all agencies to undertake immediate responsibility for executing essential agreements and updating POA&Ms to facilitate not only TIC preparations, but also due diligence for integrating the National Cyber Protection System (NCPS, operationally referred to as EINSTEIN) deployments and synchronizing with US-CERT," and OMB Memorandum M-15-01, "Fiscal year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices" requires Departments and Agencies (D/As) to enter into legally sufficient agreements with DHS relating to the deployment of EINSTEIN. DHS establishes these agreements with D/As authorizing in-line traffic inspection and modification, and such activities may include the interception, modification, use, and disclosure of D/A traffic. As such, specific EIS data service offerings: VPNS, Ethernet Transport, PLS, IPS, Cloud services, which includes IaaS Private Cloud, Paas, and SaaS, MNS Traffic Aggregation Service, MTIPS, and IPSS, and in future implementations could include other externally routed data services(e.g. OWS, SONETS), transporting Internet, Extranet, and Inter-Agency traffic shall identify and route said government traffic through a secure DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN capabilities. . The contractor shall design, implement, and operate its services to achieve the required routing of traffic through (including delivery to and receipt of traffic from) DHS EINSTEIN Enclaves. Transport SLA KPIs are measured as if through loopbacks in EINSTEIN Enclaves. EINSTEIN Enclaves are strictly intermediate hops and shall not be considered end points for SLA measurement. These contractor-performed actions related to EINSTEIN--whether performed for DHS, GSA, or customer agencies--are intended to be assistance provided to the Secretary of DHS in accordance with 6 U.S.C. § 151.
4. In 2015, section 223 of the Federal Cybersecurity Enhancement Act of 2015 (the FCEA), Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242, Division N, Title II, Subtitle B (2015) (relevant portions codified at 6 U.S.C. §§ 151 and 151 note) created a statutory requirement for the Secretary of Homeland Security to "deploy, operate, and maintain" and "make available for use by any agency" capabilities to detect cybersecurity risks in agency network

traffic and take actions to mitigate those risks. 6 U.S.C. § 151(b)(1). The FCEA also mandated that agencies deploy these capabilities fully on all perimeter network traffic. FCEA § 223(b) (6 U.S.C. § 151, note) ("[T]he head of each agency shall apply and continue to utilize the [above authorized intrusion detection and prevention] capabilities to all information traveling between an agency information system and any information system other than an agency information system."). To help enable these capabilities, the FCEA authorized DHS to "enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy, operate, and maintain technologies in accordance with [6 U.S.C. § 151(b)]"—the legal provision authorizing the capabilities. 6 U.S.C. § 151(c)(2). And, it provided that "[n]o cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to [6 U.S.C. § 151(c)(2].

5. In accordance with 6 USC 151(e)(1)(B), the contractor may not use any network traffic transiting or traveling to or from an agency information system to which the contractor gains access in accordance with 6 USC 151 for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to 6 U.S.C. § 151 (c)(2) or as part of another contract with DHS.
6. The contractor shall comply with DHS policies and procedures supplied by DHS, including those governing the operation of the intrusion detection and prevention capabilities provided pursuant to this contract, including DHS information handling guidelines regarding information obtained through operation of the intrusion detection and prevention capabilities provided pursuant 6 U.S.C. § 151.
7. The contractor shall verify in writing with DHS before providing EINSTEIN related capabilities, including as part of MTIPS, IPSS, MSS and Traffic Aggregation task orders to an Agency, that the Agency has signed the required Memorandum of Agreement (MOA) relating to deployment of EINSTEIN with DHS. This MOA is a legal requirement for DHS furnished capabilities which include EINSTEIN.

Telecommunications policy and the national telecommunications infrastructure are increasingly impacted by the convergence of telecommunications and information technology. Thus, policy directives in the areas of Electronic Government ("E-Gov"), Enterprise Architecture development, and Information Assurance, for example, may also have implications for telecommunications infrastructure. Additional policy requirements may be identified to the contractor. If contract modifications are required to meet new government-specific requirements, the contractor shall submit a technical

approach and schedule for proposing these modifications to the CO per contract modification guidelines identified in Section J.4.

C.1.8.9 Technical Support

The contractor shall provide customer technical support as a component of each of its EIS services. For detailed requirements, please see Section G.6.2 Customer Service Office and Technical Support and Section G.6.4 Trouble Ticket Management.

C.2 Technical Requirements

C.2.1 Data Service

C.2.1.1 Virtual Private Network Service

C.2.1.1.1 Service Description

The contractor's Virtual Private Network Service (VPNS) shall provide secure, reliable transport of agency applications across the provider's high-speed unified multi-service IP-enabled backbone infrastructure.

C.2.1.1.1.1 Functional Definition

The main characteristic of VPNS is that all infrastructure and devices involved in implementing the VPN are owned by the contractor and located at the edge of the contractor's backbone. Tunnels terminate at the contractor's edge router.

The contractor shall use its backbone to establish three basic solutions for VPNS:

1. Intranet ─ provides secure tunnels between remote sites, using broadband or dedicated access.
2. Extranet ─ enables trusted business partners to gain access to corporate information via secure/encrypted tunnels, using broadband or dedicated access.
3. Remote Access ─ enables mobile/remote workers to gain access to secure corporate information via secure encrypted tunnels, such as IPsec and TLS.

The contractor shall accommodate and optimize an agency's applications to enable the network to accurately and consistently allow for traffic prioritization and cost efficiencies to support the following VPNS traffic types:

1. Time-critical traffic such as voice and video.
2. Business-critical traffic such as transactions.
3. Non-critical traffic such as email.

C.2.1.1.1.2 Standards

VPNS shall comply with the following standards.

1. OMB M-11-11 “Continued Implementation of Homeland Security Presidential Directive (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors”
2. NIST Special Publication (SP) 800-46 Revision 1 “Guide to Enterprise Telework and Remote Access Security”
3. IETF RFCs:
    a) For secure VPNs:
        i. General IPSec
        ii. ESP and AH
        iii. Key exchange
        iv. Cryptographic algorithms to include but not limited to 3DES, RC4 and AES
        v. IPSec policy handling
        vi. IPSec MIBs
        vii. Remote access
        viii. Certification Authorities
    b) For trusted VPNs:
        i. General MPLS
4. IP Security Working Group – RFC 4303
5. IP Security Policy Working Group – RFC 3586
6. MPLS Working Group – RFC 3468
7. Layer 3 Virtual Private Network (L3VPN) Working Group – RFC 4176
8. Pseudo Wire Emulation Edge to Edge (pwe3) Working Group – RFC 3985
9. Use of PE-PE GRE or RFC4364 VPNs
10. IETF-TLS Working Group – RFC 5246 for TLS 1.2
11. TLS 1.2 Protocol Specification
12. IETF RFCs for IPv4 and IPv6
13. CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information Among National Security Systems

14. All new versions, amendments, and modifications to the above documents and standards

C.2.1.1.1.3 Connectivity

VPNS shall connect government locations and trusted business partners for site-to-site access or broadband for remote access to provide direct connectivity between all sites as a partially- or fully-meshed WAN.

C.2.1.1.1.4 Technical Capabilities

The following VPNS capabilities are mandatory unless marked optional.

1. The contractor shall meet applicable routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.
2. The contractor shall provide multiple tunneling standards, as required by an agency. Examples include L2TP, GRE, IP-in-IP, MPLS, IPSec, and TLS.
3. The contractor shall provide various encryption levels, as required by an agency. Examples include 3DES, RC4 and AES in accordance with the appropriate FIPS publications and modules.
4. The contractor shall provide authentication services as required by an agency. Examples include RADIUS, Internal LDAP, token integration, PKI, and X.509 certificates.
5. The contractor shall support IPv4 as both the encapsulating and encapsulated protocol.
6. The contractor shall support IPv6 as both the encapsulating and encapsulated protocol.
7. The contractor shall support QoS in the following standardized modes:
   a) Best effort
   b) Aggregate Customer Edge (CE) Interface level QoS (“hose” level)
   c) Site-to-site level QoS (“pipe” level)
   d) Intserv (RSVP) signaled
   e) Diffserv marked
8. The contractor shall support QoS across a subset of the access networks as listed below:
   a) 802.1p Prioritized Ethernet
   b) MPLS-based access

c) Multilink Multiclass PPP
d) QoS-enabled wireless:
    i. LTE
    ii. Wireless 802.11.x
    iii. Cable high-speed access (DOCSIS 1.1)
    iv. QoS-enabled Digital Subscriber Line (DSL)
    v. QoS-enabled Satellite Broadband Access

9. The contractor shall support one or more of the following application level QoS objectives:
    a) Intserv model for selected individual flows
    b) Diffserv model for aggregated flows
10. The contractor shall provide isolation of traffic and routing service that isolates the exchange of traffic and routing information to only those sites that are authenticated and authorized members of a VPN. The contractor shall provide layered security architecture to ensure that attackers will not find a single point of entry but will be faced with multiple layers of security.
11. The contractor shall support multiple VPNs by allowing both permanent and temporary access to one or more VPNs for authenticated users across a broad range of access technologies.
12. The contractor shall provide secure routing services to provide full routing capability on the VPN platform with a secure policy across the VPN.
13. The contractor shall support the inclusion of encryption, decryption, and key management profiles as part of the security management system.
14. The contractor shall support an agency in deploying its own internal security mechanisms in addition to those deployed by the contractor, in order to secure specific applications or traffic at a granularity finer than a site-to-site basis.
15. The contractor shall allow an agency to choose from alternatives for authentication of temporary access users. Authentication server choices include:
    a) Contractor-provided
    b) Third party
    c) Agency-provided

C.2.1.1.2 Features

The VPNS features are mandatory unless marked optional.

ID Number	Name of Feature	Description
1	High availability options	The contractor shall provide the following high availability options: 1. Load sharing 2. Fail-over protection 3. Diverse access points to service provider's POP(s).
2 (optional)	Interworking Services	The contractor shall provide interworking services for an agency's VPN to transparently access agency locations that use the contractor's Ethernet Transport Service.

C.2.1.1.3 Interfaces

These UNIs at the SDP for VPNS are mandatory unless marked optional.

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type (See Note 1)
1	Ethernet Interface	1 Mbps up to 10/40/100 Gbps (Std IEEE802.3ae and 802.3ab)	IPv4/v6 over Ethernet
2	Private Line Service	1. DS0 2. T1 3. T3 4. OC-3c 5. OC-12c 6. OC-48c 7. OC-192c 8. OC-768c (optional)	IPv4/v6 over PLS
3	IP over SONET Service	1. OC-3c 2. OC-12c 3. OC-48c 4. OC-192c 5. OC-768c (optional)	IP/PPP over SONET
4	DSL Service	xDSL access at 1.5 to 6 Mbps uplink, and 384 Kbps to 50 Mbps downlink	Point-to-Point Protocol, IPv4/v6
5 (optional)	Cable high speed access	256 Kbps up to 150 Mbps (Standard DOCSIS 3.0)	Point-to-Point Protocol, IPv4/v6
6	Wireless Access	1. Wi-Fi 2. LTE 3. Satellite	Point-to-Point Protocol, IPv4/v6

Notes:

1. IPv6 shall be supported by the contractor.
2. Where E-1/E-3 carrier service is provided, appropriate corresponding payload data rates apply.

C.2.1.1.4 Performance Metrics

The performance levels and acceptable quality level (AQL) of KPIs for VPNS are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Latency (CONUS)	Routine	70 ms	≤ 70 ms	See Note 1
Latency (OCONUS)	Routine	150 ms	≤ 150 ms	See Note 2
Av(VPN)	Routine	99.9%	≥ 99.9%	See Note 3
	Critical	99.99%	≥ 99.99%	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Latency value is the average round trip transmission between agency premises routers for an VPN with all of its CONUS sites. The latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. Relevant standards are RFC 1242 and RFC 2285. The contractor may propose to the government more cost-effective test and measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.
2. Latency value is the average round trip transmission between agency premises routers for an IP VPN with its CONUS and OCONUS sites. The latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. Relevant standards are RFC 1242 and RFC 2285. The contractor may propose to the government more cost-effective test and measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.
3. VPN availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the VPN is operationally available to the agency. Availability is computed by the standard formula:

$$Av(VPN) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

4. See Section G.8.2 for the definitions and measurement guidelines.

C.2.1.2 Ethernet Transport Service

C.2.1.2.1 Service Description

Carrier Grade Ethernet transport service shall be implemented over an MPLS backbone, where Ethernet links are transported using MPLS label switched paths (LSPs) inside an outer MPLS "tunnel." Point-to-point connections can also be provided by Ethernet over SONET solutions.

Ethernet Transport Service (ETS) allows agencies to interconnect their LANs (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 Gbps) transparently over the Metro Area Networks (MAN) and the Wide Area Networks (WAN) regardless of the geographical location of their sites. Ethernet Transport Service enables Intranet and Extranet services, as well as intra- and inter-agency communications.

Ethernet shall be provided as a dedicated service or a shared service. Dedicated Ethernet is defined as private services that are carried over dedicated facilities at fixed and predetermined speeds. Shared Ethernet is defined as statistically multiplexed Ethernet connections.

C.2.1.2.1.1 Functional Definition

ETS provides point-to-point, point-to-multipoint and multipoint-to-multipoint connections. ETS exploits Ethernet's flexibility, cost effectiveness, and differentiation of service (e.g., traffic priority) capabilities while providing end-to-end transport of data traffic with minimal protocol conversion. The following ETS shall be supported:

1. **Ethernet Private Line (E-LINE)**. E-Line is a point-to-point service in which bandwidth is reserved. E-Line supports full port speeds (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 or higher Gbps) and can support different quality of service (QoS) priorities for customer traffic. E-Line is a point-to-point configuration as a Layer 2 tunnel providing a transparent dedicated connection between two sites. This service resembles/replaces traditional Time Division Multiplexing (TDM) private line service. Some applications include router interconnect, business continuity, and disaster recovery. E-LINE service can be offered over the MAN and/or WAN.
2. **Ethernet Private LAN (E-LAN**). E-LAN supports both point-to-multipoint and multipoint-to-multipoint configurations. For point-to-multipoint configurations, ETS connects three or more sites over Layer 2 tunnels. It supports full port speeds (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 or higher Gbps) and can support different QoS priorities for customer traffic. For multipoint-to-multipoint configuration, also called E-Tree service, ETS connects several sites, similar to point-to-multipoint configuration, by connecting one or more roots and a set of

leaves, but preventing inter-leaf communication. More than one site can be configured as the root site and other sites can communicate with each other through multiple root sites; for example, connecting disparate LAN segments into a single agency-wide virtual LAN. E-LAN can be offered over the MAN and/or WAN.

C.2.1.2.1.2 Standards

ETS shall comply with the following standards:

1. Metro Ethernet Forum (MEF CE 2.0):
   a) (Optional) Support Jumbo Ethernet frames
   b) CE 2.0 is set of MEF CE 2.0 Certified network elements that connect to transport Carrier Ethernet services for all users, locally and worldwide. Ethernet transport services are carried over physical Ethernet networks and other legacy transport technologies.
   c) Key Specifications:
      - MEF 6.1 - CE Service Definitions
      - MEF 10.2 - CE Service Attributes
      - MEF 33 - Ethernet Access Services
      - MEF 23.1 - Class of Service
      - MEF 26.1 - ENNI
   d) CE 2.0 expands CE 1.0 to:
      - 8 services, 2 of each respectively in E-Line, E-LAN, E-Tree, and E-Access (defined in MEF Standards MEF 6.1, 22.1, 33)
      - Standardized Multi-CoS with application-oriented CoS Performance Objectives, new metrics (MEF 6.1, 10.2, 20, 23.1)
      - Interconnect through the integrated delivery of MEF Service Attributes (MEF 10.2, 26.1, 33) allows ubiquitous deployment spanning multiple providers
      - Manageability, (MEF 7.1, 16, 17, 30, 31) plus additional specifications
2. International Telecommunications Union (ITU):
   a) *Network architecture*:
      - G.8010/Y.1306 Architecture of Ethernet layer networks
   b) *Services:*
      - G.8011/Y.1307 Ethernet over Transport – Ethernet services framework

- G.8011.1/Y.1307.1 Ethernet private line service
- G.8011.2/Y.1307.2 Ethernet virtual private line service
- G.8011.3/Y.1307.3 Ethernet virtual private LAN service (draft)
- G.8011.4/Y.1307.4 Ethernet virtual private rooted multipoint service (draft)
- G.8012/Y.1308 Ethernet UNI and Ethernet NNI

c) *OAM*:

- Y.1730 Requirements for OAM functions in Ethernet-based networks and Ethernet services
- Y.1731 OAM functions and mechanisms for Ethernet-based networks

d) *Protection:*

- G.8031/Y.1342 Ethernet linear protection switching
- G.8032/Y.1344 Ethernet ring protection switching

e) *Equipment:*

- G.8021/Y.1341 Characteristics of Ethernet transport network equipment functional blocks

f) *Equipment management:*

- G.8051/Y.1345 Management aspects of the Ethernet-over-Transport (EoT) capable network element

g) *Terminology:*

- G.8001/Y.1354 Terms and definitions for Ethernet frames over Transport (EoT)

3. Institute of Electrical and Electronics Engineers, Inc. (IEEE):
   a) IEEE 802.3, 1Gbps LAN PHY, 10Gbps LAN PHY, 10Gbps WAN PHY
   b) IEEE 802.3ae, 10Gbit Ethernet 802.17, Resilient Packet Rings (RPR) – in progress
   c) IEEE 802.1ah, Ethernet First Mile
   d) IEEE 802.1p
   e) IEEE 802.1q
4. Acceptance Testing of ETS:
   a) RFC 2544
   b) RFC 6815
5. All new versions, amendments, and modifications to the above documents and standards

C.2.1.2.1.3 Connectivity

ETS shall connect to and interoperate with:

1. **Intra-agency LAN-LAN Connectivity.** ETS provides connectivity for an agency's LANs located in the same city or different cities, thereby extending the LAN to the MAN and WAN. This is achieved by connecting the agency's SDP(s) in one location to another SDP(s) in one or more locations. Interconnection shall be possible over transoceanic links, if required.
2. **Inter-agency LAN-LAN Connectivity**. Different agencies may share resources to connect to the contractor's metro or long haul network. This is achieved by connecting from one agency's SDP(s) to other agencies' SDP(s).

C.2.1.2.1.4 Technical Capabilities

The following ETS capabilities are mandatory unless marked optional:

1. The contractor shall meet applicable routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.
2. Geographical Coverage. A seamless end-to-end service shall be provided from the SDP Customer Premise Equipment (CPE) traversing the contractor's network (Metro Access/Core and Long Haul) in order to minimize conversion of protocols. The contractor shall indicate if protocol conversions are required and how they impact the delay when delivering services end-to-end. The following geographical coverage shall be provided:
   a) Intra-City ETS – the contractor shall provide Ethernet connections to agency sites located in the same city inside the US (CONUS and Metro) and outside the US (OCONUS and Non-Domestic).
   b) Inter-City ETS – Ethernet connections shall be delivered at domestic and non-domestic locations (CONUS/Metro, OCONUS/Non-Domestic).
3. The contractor shall support Ethernet UNI (User-to-Network-Interface) to support Layer 2 and Layer 3 clients. Layer 3 clients are agency devices that support Layer 3 protocol packets such as IPv4, IPv6.
4. The contractor shall support Ethernet Virtual Connections (EVCs).
5. The contractor shall support delivery of the ETS at the agency's Service Delivery Point (SDP) via a UNI.
6. If required, the contractor shall support circuit emulation services for TDM services.

7. The contractor shall support point-to-point, multipoint-to-multipoint, and Rooted multipoint EVCs.
8. EVC multiplexing shall be supported.
9. The contractor shall support rate-limited throughput access links, i.e., 1 Gbps port rate limited in 100 Mbps increments.
10. The contractor shall support rate-limiting at the agency's SDP and at the individual VLAN ingress and egress.
11. Privacy and security shall be supported per IEEE 802.3 as defined in the TO.
12. The contractor shall support the following service attributes:
    a) Physical interfaces shall be supported as listed in Section C.2.1.2.3
13. The following traffic profiles shall be supported:
    a) Committed Information Rate (CIR) – minimum amount of bandwidth guaranteed for an ETS
    b) Committed Burst Size (CBS) – the size up to which subscriber traffic is allowed to burst and still be in-profile and not discarded or shaped
    c) Peak Information Rate (PIR) – specifies the rate above the CIR that traffic is allowed into the network for a given burst interval defined by the MBS
    d) Maximum Burst Size (MBS)
14. Performance parameters shall be supported as listed in Section C.2.1.2.4.
15. Service Frame Delivery options supported shall include:
    a) Unicast Frame Delivery
    b) Multicast Frame Delivery, as per RFC 4604
    c) Broadcast Frame Delivery as per IEEE 802.3
16. VLAN tag supported shall include:
    a) VLAN tag preservation
    b) VLAN tag translation
    c) VLAN tag stacking
    d) VLAN aggregation across a common physical connection (optional)
17. Service multiplexing shall be supported to include multiple EVCs connected via a single UNI.
18. Bundling shall be supported to enable two or more VLAN IDs to be mapped into a single EVC at a UNI.

19. Security Filters shall be supported as specified in the TO.
20. (Optional) The contractor shall provide proactive Performance Monitoring (PM). It is desirable that all items in the following list be supported:
    a) Signal failure
    b) Signal degradation
    c) Connectivity or Loss of connectivity
    d) Frame loss
    e) Errored frames
    f) Looping
    g) Denial of service (DoS)
    h) Misinserted frames
    i) Maintenance parameters
21. The contractor shall support the following maintenance functions:
    a) Alarm suppression
    b) Loopbacks (intrusive and non-intrusive (transparent to on-going connections))
    c) Protection switching, restoration, etc.
22. The contractor shall support the following network topologies:
    a) Point-to-point
    b) Rooted Multipoint
    c) Multipoint-to-Multipoint (i.e., mesh)
23. The contractor shall support geographical diversity to provide added reliability. An agency may buy a geographical diverse route from the same or a different contractor to serve as a protection path.
24. The contractor shall support bridging in compliance with IEEE 802.1Q (2014).
25. The contractor shall support the following Virtual Connection sizes:
    a) For point-to-point Ethernet connections – up to 40 Gbps
    b) For multi-point-to-multi-point connections – up to 40 Gbps
26. Quality of Service (QoS) – The contractor shall support traffic prioritization that enables higher priority traffic to be transmitted first.
27. The contractor shall support traffic reconfiguration that supports the ability of the agency to modify a specific service connection subsequent to the establishment of the connection. Changes to an established connection may include upgrade/downgrade of speeds that do not result in physical equipment changes.

C.2.1.2.2 Reserved

C.2.1.2.3 Interfaces

The UNIs at the SDP are mandatory unless marked optional:

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling Protocol Type/Granularity
1	Optical	IEEE 802.3z	1310 nm	1 Gbps	Gigabit Ethernet
2	Optical	IEEE 802.3z	850 nm	1 Gbps	Gigabit Ethernet
3 (optional)	Optical	IEEE 802.3	1310 nm	100 Mbps	Fast Ethernet
4 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm	10/40/100 Gbps	10/40/100GBASE-SR (65 meters)
5 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	850nm	10/40/100 Gbps	10/40/100GBASE-SW
6 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1550 nm	10/40/100 Gbps	10/40/100GBASE-ER
7 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm	10/40/100 Gbps	10/40/100GBASE-LR
8 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1550 nm	10/40/100 Gbps	10/40/100GBASE-LW

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling Protocol Type/Granularity
9 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1300 nm Multimode	10/40/100 Gbps	CWDM 10/40/100GBASE-LX4 (300 meters)
10 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm Single Mode	10/40/100 Gbps	CWDM 10/40/100GBASE-LX4 (10,000 meters)
11 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm Single Mode	10/40/100 Gbps	10/40/100GBASE-LW (10,000 meters)
12 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1550 nm Single Mode	10/40/100 Gbps	10/40/100GBASE-EW (40,000 meters)
13 (optional)	Electrical	IEEE 802.3	N/A	10 Mbps	10Base
14	Electrical	IEEE 802.3	N/A	100 Mbps	100 Base
15	Optical	IEEE 802.3		1 Gbps	1000Base
16 (optional)	Optical	ITU-T G.707	1300 nm	STM-4	SDH STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4
17 (optional)	Optical	ITU- G.707	1300 nm	STM-4c	VC-4-4c
18 (optional)	Optical	IEEE 802.3z IEEE 802.3ab	Multimode	1 Gbps	1000BASE-LX

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling Protocol Type/Granularity
19 (optional)	Optical	IEEE 802.3z IEEE 802.3ab	Multimode	1 Gbps	1000BASE-SX
20 (optional)	Electrical (Copper)	IEEE 802.3z	N/A	1 Gbps	1000BASE-CX
21 (optional)	Electrical (Twisted pair)	IEEE 802.3z	N/A	1 Gbps	1000BASE-T
22 (optional)	Optical	GR-253, ITU-T G.707	1310 nm	10/40 Gbps	SONET or SDH

C.2.1.2.4 Performance Metrics

The performance levels and AQL of KPIs for ETS are mandatory unless marked optional:

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Av (ETS)	Routine (Single Connection)	99.9%	≥ 99.9%	See Note 1
	Critical (Double Connection)	99.99%	≥ 99.99%	
Latency (ETS)	CONUS	100 ms	≤ 100 ms	See Note 2
	OCONUS	200 ms	≤ 200 ms	
Jitter (Packet)	Routine	10 ms	≤ 10 ms	See Note 3

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Grade of Service (Packet Delivery)	Routine	99.95%	≥ 99.95% at all times	See Note 4
	Critical	99.99%	≥ 99.99% at all times	
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 5
	With Dispatch	8 hours	≤ 8 hours	
Grade of Service (Fail Over Time)	Routine	1 minute	1 minute	See Note 6
	Critical	100 ms	≤ 100 ms	See Note 6

Notes:

1. ETS availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the ETS is operationally available to the agency. Availability is computed by the standard formula:

$$Av(EthS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Latency is the round trip delay experienced by an end user across the contractor's network to other agencies' sites. It is the average time for packets to travel over the core network. The Internet Control Message Protocol (ICMP) test can be used to calculate packet delivery and latency. The ICMP test consists of sending, every five minutes, a series of five test packets between originating agency's SDPs and the delivery SDPs. The test results are analyzed to determine packet loss vs. successful delivery and speed of delivery. Contractor shall meet or exceed standards set by RFC 1242 and RFC 2285. It can be determined by the following formula: (Distance/(0.6*c)+hops*delay), where c is the velocity of light and 0.6 is the multiplier recommended by the ITU (G.144) in

ms/km plus the delay in each hop caused by the routers times the number of hops.

3. Measurements of packet jitter are performed by injecting packets at regular intervals into the network and measuring the variability in the arrival time. Relevant standard is RFC 2679.
4. Network devices, such as switches and routers, sometimes have to hold data packets in buffered queues when a link gets congested. If the link remains congested for too long, the buffered queues will overflow and data will be lost. The loss can be measured with the ICMP test. The contractor is expected to meet or exceed relevant standards such as RFC 1242 and RFC 2285.
5. As per GR-418. Refer to Section G.8.2 for definitions and how to measure.
6. Restoration for links transported over the Ethernet infrastructure (i.e., Ethernet switches) is achieved by the use of protocols such as Spanning Tree (IEEE 802.1d), which converge more slowly than SONET. Therefore, ETS for critical users shall be delivered over a carrier class infrastructure.

C.2.1.3 Optical Wavelength Service

Government agencies require dedicated broadband, framing-independent transport networks to interconnect their offices in different regions of the United States and internationally. In offering Optical Wavelength Service (OWS), the contractor always provides the optical electronics (optronics) equipment and fiber connectivity that comprise the transport network. Management of the network, however, may be performed by either the contractor or the agency. In the latter case, agencies will manage their dedicated networks via a Web portal or a remote user interface.

C.2.1.3.1 Service Description

The method of providing OWS is Wavelength Division Multiplexing (WDM).

OWS delivered over WDM provides a high-bandwidth solution without the cost of owning and operating network infrastructure.

OWS is provided over WDM equipment where several wavelengths, or lambdas, are multiplexed into a composite signal that is transported over a single fiber. The composite signal is then de-multiplexed at the receiver end and each wavelength is recovered.

C.2.1.3.1.1 Functional Definition

Basic OWS is a point-to-point, bi-directional, single link service delivered over WDM.

C.2.1.3.1.2 Standards

OWS over WDM shall comply with the following standards, as applicable:

1. ITU Standards defining frequencies grid and physical layer parameters for WDM are G.692 and G.694.
2. ITU Standards defining frequencies grid for CWDM are G.694.2.
3. (Optional) ITU Standards defining OTN architecture, interface formats, and physical layer interfaces are G.872, G.709, and G.959.1 respectively.
4. Applicable ITU Standards defining submarine transmission functional requirements are G.971, G.972, G.973, G.974, G.975, G.976 and G.977.
5. Telcordia standards for metro and long haul protection are GR-253, GR-1400, and GR-1230.
6. Telcordia standard for reliability assurance is GR-418.
7. Applicable Telcordia for WDM systems are GR-1073, GR-1312, GR-2918, GR-2979 and GR-3009.
8. VSR4-01 (OC-192 Very Short Reach Interface, 12 fibers 850nm)
   OIF-VSR4-01.0 - Very Short Reach (VSR) OC-192 Interface for Parallel Optics (optional).
9. VSR4-02 (OC-192 Very Short Reach Interface, 1 fiber 1310nm)
   Note: VSR4-02 has been included as the 4dB link option in VSR4-05 below (optional).
10. VSR4-03.1 (OC-192 Very Short Reach Interface, 4 fibers 850nm)
    OIF-VSR4-03.0 - Very Short Reach (VSR) OC-192 Four Fiber Interface Based on Parallel Optics (optional).
11. VSR4-04 (OC-192 Very Short Reach Interface, 1 fiber 850nm)
    OIF-VSR4-04.0 - Serial Shortwave Very Short Reach (VSR) OC-192 Interface for Multi-mode Fiber (optional).
12. VSR4-05 (OC-192 Very Short Reach Interface, OXC 1310nm)
    OIF-VSR4-05.0 - Very Short Reach (VSR) OC-192 Interface Using 1310 Wavelength and 4 and 11 dB Link Budgets (optional).
13. VSR5-01 (OC-768 Very Short Reach Interface)
    OIF-VSR5-01.0 - Very Short Reach Interface Level 5 (VSR-5): OWS OC-768 Interface for Very Short Reach (VSR) Applications (optional).

14. All new versions, amendments, and modifications to the above documents and standards.

C.2.1.3.1.3 Connectivity

OWS shall be delivered at the Service Delivery Point (SDP) via UNIs as specified in Section C.2.1.3.3.

Point-to-point, bi-directional, duplex services shall be connected from the SDP to the Optical Transport Network via a fiber pair.

The wavelengths ordered by the agencies shall connect to and interoperate with:

1. Contractor's metro and long haul networks
2. Agency's Intranet
3. Other agency networks

C.2.1.3.1.4 Technical Capabilities

The following OWS capabilities are mandatory unless marked optional:

The contractor shall support the following three types of connections:

1. **Non-domestic Wavelengths (optional)**. The contractor shall support international wavelengths that may be part of an end-to-end service or a stand-alone connection. An end-to-end wavelength service shall drop and pick up traffic from and to locations, as required by an agency:
   a) Backhaul services shall be available where necessary.
   b) The basic service shall be a single point-to-point; bi-directional wavelength connecting two sites.
2. **Domestic Wavelengths**. The contractor shall support wavelengths over the long-haul network. This is applicable for inter-city connectivity within the United States and territories not in the continental US.

   The basic service shall be a single point-to-point, bi-directional wavelength connecting two agency sites located in different states.
3. **Metro Wavelength Services**. The contractor shall support the provisioning of wavelengths over its metro networks.

   Single point-to-point, bi-directional wavelengths connecting two agency sites in the same city shall be supported.

The contractor shall provide the following capabilities:

1. **Transmission Rates**. Wavelengths shall be supported at 1 Gbps, 2.5 Gbps, and 10 Gbps. The contractor has the option to also support wavelengths at 40 Gbps and 100 Gbps. Following the implementation of EIS, the contractor may support additional optional rates beyond 100 Gbps if and when such transmission rates become available.
2. **Clock Transparency**. The contractor's networks shall support the following levels of clock transparency:
   a) Asynchronous transport, where the contractor's network shall not apply clocking to the agency's traffic
   b) The contractor's network shall provide Synchronous Status Messaging (SSM) byte transparency
3. **Protocol Transparency - Metro**. The contractor shall support Metro wavelengths that are rate and protocol independent.
4. **Protocol Transparency – Domestic and Non-Domestic**. The contractor shall support Domestic and Non-Domestic Wavelengths that are rate and protocol independent. (optional)
5. **Byte Transparency**. The support to framed wavelengths shall include byte transparency where the overhead bytes are passed through without being overwritten (i.e. non-intrusive Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) processing of the signals).
   a) Transparency of Transport Overhead (TOH) bytes shall be provided, with the exception of A1 and A2 bytes, B0 and J1. A1 and A2 are framing bytes which monitor the framing integrity of the incoming Synchronous Transport Signal Level-N (STS-N, where N=1, 3, 12, 48, 192, 768) and Optical Carrier Level-N (OC-N, where N=1, 3, 12, 48, 192, 768) signals. The framing bytes can be terminated.
   b) If the framed wavelengths supported are not fully transparent, the contractor shall indicate the level of transparency offered for wavelengths at 2.5 Gbps, 10 Gbps and 40 Gbps.
   c) Fully transparent wavelengths shall be supported at 40 Gbps. This applies to Non-domestic, domestic, and metro wavelengths.
6. **Concatenation**. For framed wavelengths, the contractor shall support standard and virtual concatenation.
7. **(Optional) Channelization.** For framed wavelengths, the contractor shall support channelized UNIs.

8. **Wavelength Delivery.** Hand-off at the SDP shall be accomplished using two fibers over two ports when delivering bidirectional wavelength services, with one fiber for each direction. Patch panel and fiber terminations will be based on agency needs.
9. **Access Methods**. The contractor shall provide access methods to the ordered wavelength service for an end-to-end offering.
    a) If the contractor is not able to provide access on its network, it shall indicate what alternatives exist to enable the service end-to-end.
    b) Each end of the wavelength shall be delivered using access methods as required by the agency.
    c) When agency access is provided via the backbone of the Long Haul (LH) DWDM systems and is not collocated, the contractor shall specify the appropriate reach of the optical interface to be used. If the distance is too long for interfaces such as FICON, Fibre Channel, etc., the mediation devices or gateways needed shall be specified in order to compensate for distance limitations.
10. **Government Furnished Property (GFP) / SRE**. The contractor shall provide multi-vendor interoperability support to the GFP/SRE by completing connectivity using the appropriate UNIs in the following cases:
    a) Should the GFP/SRE and the metro WDM system be collocated at the agency's office, connectivity between them shall be established using Short Reach (SR) interfaces (1310 nm) or Very Short Reach (VSR).
    b) Should the GFP/SRE and the metro WDM systems be not collocated; the metro WDM shall be located in a telehouse or collocation hotel. In this case, the contractor shall interface with the GFP/SRE using the appropriate optical interface that shall reach the distance between the agency's office and the collocation site.
    c) The wavelength service shall be able to support different kinds of traffic depending on the type of GFP/SRE (i.e., Fiber Connectivity (FICON), Enterprise System Connection (ESCON), and Fibre Channel for a Storage Area Network (SAN)).
11. **Efficient Transport**. The contractor shall ensure that a single wavelength is capable of transporting different types of traffic without the need to use a separate physical wavelength to run IP, Ethernet, etc.

C.2.1.3.2 Features

The following Optical Wavelength Service (OWS) over WDM features are mandatory, unless marked optional:

ID Number	Name of Feature	Description
1 (Optional)	Customer Network Management (CNM) – Level 1	The contractor shall provide monitoring capabilities only via this feature. Agency personnel shall be able to monitor wavelength(s) via alarm messages from the Optical Transport Network into a software user interface via a dashboard or an API from the agency network management system.
2 (Optional)	Customer Network Management (CNM) – Level 2	The contractor shall provide management and monitoring capabilities. These shall be included to support an alarm messages visibility and execution of control commands that shall be sent into the wavelength(s). Operations available shall include set up, modification and tearing-down connections.
3	Equipment Protection 1:1 – GFP/SRE	The contractor shall provide protection to the client interfaces at the SDP, where the protection channel is bridged to the failed working channel.
4	Equipment Protection 1+1 – GFP/SRE	The contractor shall provide protection to the User to Network Interfaces at the SDP, where the protection channel is permanently bridged to the working channel. Protection switching is faster than 1:1.
5	Equipment protection – Network Side	The contractor shall support two channels facing the network for full redundancy and equipment protection at the SDPs.
6	Geographical Diversity Wavelengths	The contractor shall support geographically diverse wavelengths to be used by the agency as a hard protection against fiber failures. The configuration and exact diversity requirements, such as single/dual site delivery, single or dual metro hub, will be specified in the TO.
7 (Optional)	Protected Non-Domestic and OCONUS Wavelength	The contractor shall support protected Non-Domestic and OCONUS Wavelengths. These shall be architected using submarine transmission protocols such as Bidirectional Path Switched Ring (BPSR) or equivalent. The contractor shall ensure protection switching in the submarine transmission networks to be less than 4 seconds for a single failure.

ID Number	Name of Feature	Description
8 (Optional)	Protected CONUS Wavelength	The contractor shall support protected CONUS Wavelengths using transmission protocols to provide resiliency. Protection switching in the nationwide transmission networks shall be less than 300 ms for a single failure. This feature is limited to 2,500 kilometers.
9	Protected Metro Wavelength	The contractor shall provide protection on a per-wavelength basis when delivering services in the metro areas, such as Unidirectional Path Switched Ring (UPSR). Restoration times for protected wavelengths in the metro area shall be below 60 ms for a single failure. When delivering protected wavelengths in the metro area, the agency and the contractor shall agree on whether equipment protection is required facing the GFP/SRE. If so, the contractor shall provide protection at the SDP and multiple UNIs shall be ordered, the number of which shall depend on the protection method selected by the agency. The contractor shall supply its own physical UNIs.

C.2.1.3.3 Interfaces

The existing UNIs at the SDP are mandatory unless marked optional:

UNI Type	Interface Type	Standard	Frequency of Operation	Payload Data Rate or Bandwidth	Signaling or Protocol Type
1	Optical	GR-253, ITU-T G.707	1310 nm	2.5Gpbs	SONET or SDH
2	Optical	GR-253, ITU-T G.707	1310 nm	2.5Gbps	SONET or SDH Concatenated
3	Optical	GR-253, ITU-T G.707	1310 nm	10Gbps	SONET or SDH
4 (optional)	Optical (over 12 fibers)	OIF-VSR4-01.0	850 nm	10 Gbps (12 fibers)	SONET or SDH

UNI Type	Interface Type	Standard	Frequency of Operation	Payload Data Rate or Bandwidth	Signaling or Protocol Type
5 (optional)	Optical (over 1 fiber)	OIF VSR4-02	1310nm	10 Gbps (1 fiber)	SONET or SDH
6 (optional)	Optical (over 4 fibers)	OIF-VSR4-03.0	850nm	10 Gbps (4 fibers)	SONET or SDH
7 (optional)	Optical (over 1 fiber)	OIF-VSR4-04.0	850 nm	10 Gbps (1 fiber)	SONET or SDH
8 (optional)	Optical	OIF-VSR5-01.0	850 nm	40 Gbps	SONET or SDH

C.2.1.3.4 Performance Metrics

1. Framed Wavelength Performance – Wavelengths based on SONET framing shall comply with performance requirements as stated in Section C.2.1.5.1.4 (7) through (8).
2. Transparent Wavelength Performance – If applicable, the contractor shall describe the methods by which fully transparent wavelengths (i.e. based on all optical gear, G.709 based) will be monitored and how AQLs will be met.
3. The contractor shall support In-Service Monitoring (ISM) and shall not rely on performance observed and measured at higher layers of the network.

The Performance Levels and AQL of KPIs for OWS over WDM are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Av(OWS over WDM)	Routine	99.9%	≥ 99.9%	In-Service Monitoring See Note 1
	Critical	99.99%	≥ 99.99%	

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	
Grade of Service (Restoration Time)	Routine	100 ms	≤ 100 ms	In-Service Monitoring See Note 3
	Critical	60 ms	≤ 60 ms	

Notes:

1. OWS availability shall be measured in service on an end-to-end basis. COT(HR) shall be calculated based on errored seconds and/or severely errored seconds (SES) as defined by GR-253, G.826 through G.829 and shall be expressed in Hours. Availability is computed by the standard formula:

$$Av(OWS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section G.8.2 for definition and how to measure.
3. Restoration time is the time taken to reroute the traffic over a redundant path before the failure is repaired. For critical user traffic, the redundant path should be a geographically diverse wavelength in a 1+1 configuration where the time accounted for includes the switching time and the propagation time in the fiber. Proactive monitoring using element management systems should be used to measure restoration time in real time. Simulation tools are also available and used by contractors. Calculated based on an 8000 km ring using the following formula: T= Detect time + Time in fiber + Time in Nodes + Time to bridge and switch + Traffic delay time. Domestic networks are usually ring based on the backbone. For 1+1 protection based on APS, GR-253 compliance includes 10 ms for detection and 50 ms for the actual switching.

C.2.1.4 Private Line Service

C.2.1.4.1 Service Description

Private Line Service (PLS) provides dedicated, reliable full-duplex bandwidth for agency-specific data networks and mission critical applications. The ranges of line speeds and reliability options provided by this service allow government users to satisfy an array of diverse requirements. This service can be used for various applications such as voice, data, video, multimedia, and encrypted communications.

C.2.1.4.1.1 Functional Definition

PLS provides dedicated duplex transmission connectivity between two or more designated end points over which agency service applications traverse at agency-specified bandwidths. The connectivity between the end points is permanently established unless a service request is received for a modification, move, or disconnect.

C.2.1.4.1.2 Standards

PLS shall comply with the following standards:

1. ANSI T1.102/107/401/403/503/510 for T1
2. Telcordia PUB GR-499-CORE for T3
3. ANSI T1.105 and 106 for SONET
4. Telcordia PUB GR-253-CORE for SONET
5. ITU-TSS G.702 and related Recommendations for E1 and E3
6. Telcordia PUB SR-TSV-002275, TR-NWT-000965, and TR-NWT-000335 for analog
7. Telcordia PUB GR-418-CORE for reliability/performance

C.2.1.4.1.3 Connectivity

PLS shall connect to and interoperate with:

1. Government-specified terminations (e.g., SDPs such as PBXs, Multiplexers, Routers, Video CODECs, and Group 4 FAXs)
2. All other networks including other EIS contractors' networks, where additional coordination between networks will be required for interoperability

C.2.1.4.1.4 Technical Capabilities

The following PLS capabilities are mandatory unless marked optional:

1. The contractor shall meet applicable routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.
2. Transparency to any protocol used by GFP.
3. Data transparency treatment of all bit sequences transmitted by GFP through the SDP.

The contractor shall support the following categories (i.e., data rates) of PLS service:

1. **DS0**. Information payload data rates of 56 Kbps and 64 Kbps.
2. **T1**. Line rate of 1.544 Mbps, which may be used to provide channelized or un-channelized T1 service as follows:
   a) Channelized T1. In this mode, 24 separate DS0s clear channels of either 56 Kbps or 64 Kbps shall be supported.
   b) Un-channelized T1. In this mode, a single 1.536 Mbps information payload shall be supported.
3. **T3**. Line rate of 44.736 Mbps, which may be used to provide channelized or un-channelized T3 service as follows:
   a) *Channelized T3*. In this mode, 28 separate DS1 channels of 1.536 Mbps information payload rate shall be supported.
   b) *Un-channelized T3*. In this mode, a single 43.008 Mbps payload shall be supported.
4. **E1**.. Line rate of 2.048 Mbps, which may be used to provide channelized or un-channelized E1 service as follows:
   a) *Channelized E1*. In this mode, 30 separate DS0 clear channels shall be supported.
   b) *Un-channelized E1*. In this mode, a single 1.92 Mbps information payload shall be supported.
5. **E3**. Line rate of 34.368 Mbps, which may be used to provide channelized or unchannelized E3 service as follows:
   a) *Channelized E3.* In this mode, 16 separate E1 channels shall be supported.
   b) *Un-channelized E3* In this mode, a single 30.72 Mbps information payload shall be supported.
6. **(Optional) SONET OC-1**. Single SONET OC-1 channel with the information payload data rate of 49.536 Mbps over an interface with a line rate of 51.840 Mbps.

7. **(Optional) SONET OC-1**. Virtual Tributary. Seven Virtual Tributary (VT) groups over a single SONET OC-1 interface with a line rate of 51.840 Mbps. Each VT group shall be able to independently carry four T1 or two DS1C or one DS2 channel(s); where each T1 has a line rate of 1.544 Mbps and payload data rate of 1.536 Mbps, and each DS1C has a line rate of 3.152 Mbps and information payload data rate of 3.072 Mbps, and each DS2 has a line rate of 6.312 Mbps and information payload data rate of 6.144 Mbps.
8. **SONET OC-3**. Line rate of 155.520 Mbps, which may be used to provide channelized OC-3 or concatenated OC-3c service as follows:
    a) *Channelized OC-3*. In this mode, three separate OC-1 channels, each with an information payload data rate of 49.536 Mbps, shall be supported.
    b) *Concatenated OC-3c*. In this mode, a single channel equivalent to information payload data rate of 148.608 Mbps shall be supported.
9. **SONET OC-12**. Line rate of 622.080 Mbps, which may be used to provide channelized OC-12 or concatenated OC-12c:
    a) *Channelized OC-12*. In this mode, 4 separate OC-3 channels, each with an information payload data rate of 148.608 Mbps, shall be supported.
    b) *Concatenated OC-12c*. In this mode, a single channel equivalent to an information payload data rate of 594.432 Mbps shall be supported.
10. **SONET OC-48**. Line rate of 2.488 Gbps, which may be used to provide channelized OC-48 or concatenated OC-48c:
    a) *Channelized OC-48*. In this mode, 4 separate OC-12 channels, each with an information payload data rate of 594.432 Mbps, shall be supported.
    b) *Concatenated OC-48c*. In this mode, a single channel equivalent to an information payload data rate of 2.377728 Gbps shall be supported.
11. **SONET OC-192**. Line rate of 10 Gbps, which may be used to provide channelized OC-192 or concatenated OC-192c:
    a) *Channelized OC-192*. In this mode, 4 separate OC-48 channels, each with an information payload data rate of 2.488 Gbps, shall be supported.
    b) *Concatenated OC-192c*. In this mode, a single channel equivalent to an information payload data rate of 9.510912 Gbps shall be supported.
12. **(Optional) SONET OC-768**. Line rate of 40 Gbps, which may be used to provide channelized OC-768 or concatenated OC-768c:
    a) *Channelized OC-768*. In this mode, 4 separate OC-192 channels, each with an information payload data rate of 9.510912 Gbps, shall be supported.

b) *Concatenated OC-768c*. In this mode, a single channel equivalent to an information payload data rate of 38.486016 Gbps shall be supported.

13. **(Optional) Subrate DS0**. Information payload data rates of 4.8, 9.6, and 19.2 Kbps.
14. **(Optional) Analog Line (4KHz)**.
15. **(Optional) Fractional T1**. Two, four, six, eight, or twelve adjacent DS0 clear channels over an interface of T1 with a line rate of 1.544 Mbps.
16. **Fractional T3**. Two adjacent T1 clear channels over an interface of T3 with a line rate of 44.736 Mbps.

C.2.1.4.2 Features

The following PLS features are mandatory unless marked optional:

ID Number	Name of Feature	Description
1	Multipoint Connection	The contractor shall allow interconnection of three or more subscriber premises as follows: Branch-Off. In this mode, all SDPs shall be treated as one shared medium and each point shall be able to autonomously send and receive data. The application will ensure master/slave mode of operation (e.g., polling scheme used in IBM 3270 mode of data communication). Drop-and-Insert. In this mode, previously specified channels of a channelized T1, T3, SONET OC-3, or SONET OC-12 service category shall be able to be dropped off and new channels shall be able to be simultaneously picked up or inserted.
2	Special Routing	The contractor shall provide different routes for PLS circuits based on the following arrangements: Transport Diversity. Between connecting POPs, the contractor shall supply two or more physically separated routes for PLS circuits. These diverse routes shall not share common telecommunications facilities or offices. The contractor shall maintain a minimum separation of 30 feet throughout all diverse routes. The government recognizes that uncompromised (i.e., adhering to the minimum separation requirements as described above) diversity may not be available in some locations. Where uncompromised diversity is not available, the contractor shall exert best efforts to propose an acceptable arrangement along with documentation describing the compromise. Each pair of circuits that must be diverse from each other constitutes a relationship pair. For example, three circuits

ID Number	Name of Feature	Description
		ordered as being diverse from each other constitute three relationship pairs, i.e., 1 and 2, 1 and 3, and 2 and 3. If diversity is not available or the compromised diversity is not acceptable to the government, it shall be negotiated on an individual case basis. Transport Avoidance. Between connecting POPs, the contractor shall supply the capability for a customer to define a geographic location or route on the network to avoid. The government recognizes that avoidance may not be available in some locations. Where avoidance is not available, the contractor shall exert best efforts to propose an acceptable arrangement along with documentation describing the reasons for the unavailability. The contractor shall establish an internal control (i.e., electronic flagging of routes) to prevent accidental dismantling of diversified/avoidance routes, especially during routine route optimization initiatives by the contractor. The contractor shall provide, within 30 calendar days of the implementation of transport diversity or avoidance, and again thereafter whenever a change is made, a graphical representation (e.g., diagrams/maps) of transport circuit routes to show where diversity or avoidance has been implemented. The contractor shall provide, at least 30 calendar days in advance of implementation, written notification to the agency (with a copy to the PMO) requesting government approval of any proposed reconfiguration of routes that were previously configured for transport diversity or avoidance. When a user selects an explicit diversity and/or avoidance, the performance level of the PLS circuit will be specified by the user at the service ordering time.

C.2.1.4.3 Interfaces

The UNIs at the SDP are mandatory unless marked optional:

UNI Type	Interface Type and Standard	Payload Data Rate	UNI Type
1	ITU-TSS V.35	Up to 1.92 Mbps	Transparent
2	EIA RS-449	Up to 1.92 Mbps	Transparent
3	EIA RS-232	Up to 19.2 Kbps	Transparent
4	EIA RS-530	Up to 1.92 Mbps	Transparent

UNI Type	Interface Type and Standard	Payload Data Rate	UNI Type
5	T1 (with ESF) [Std: Telcordia SR-TSV-002275; ANSI T1.403}	Up to 1.536 Mbps	Transparent
6	T3 [Std: Telcordia GR-499-CORE]	Up to 43.008 Mbps	Transparent
7	E1 [Std: ITU-TSS G.702]	Up to 1.92 Mbps	Transparent
8	E3 [Std: ITU-TSS G.702]	Up to 30.72 Mbps	Transparent
9 (optional)	Optical: SONET OC-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	Transparent
10 (optional)	Electrical: SONET STS-1/EC-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	Transparent
11	SONET OC-3 (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
12	SONET OC-3c (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
13	SONET OC-12 (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
14	SONET OC-12c (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
15	SONET OC-48 (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
16	SONET OC-48c (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
17	SONET OC-192 (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent
18	SONET OC-192c (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent

UNI Type	Interface Type and Standard	Payload Data Rate	UNI Type
19 (Optional)	SONET OC-768 (Std: ANSI T1.105 and 106)	38.486016 Gbps	Transparent
20 (Optional)	SONET OC-768c (Std: ANSI T1.105 and 106)	38.486016 Gbps	Transparent

C.2.1.4.4 Performance Metrics

The performance levels and AQL of KPIs for PLS circuits are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability (POP-to-POP)	Routine	99.9%	≥ 99.9%	See Note 1
	Critical	99.99%	≥ 99.99%	
Availability (SDP-to-SDP)	Routine	99.9%	≥ 99.9%	
	Critical	99.99%	≥ 99.99%	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	See Note 2

Notes:

1. Availability:
   a) For data rates of T1 and higher, a service is considered unavailable when a PLS circuit experiences 10 consecutive severely errored seconds (SES) [Standard: Telcordia PUB GR-418-CORE]. An unavailable circuit is considered available when restoration activities have been completed and 30 consecutive minutes have passed without any errored seconds to account for stability and proving period. However, if there is no error second encountered during the proving period of 30 minutes, this will not be counted towards the circuit unavailable time.
   b) For data rates lower than T1, cumulative outage time is calculated based on trouble ticket data.

c) PLS availability is calculated as a percentage of the total reporting interval time that PLS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100 \ .$$

Critical level of Service for availability only applies to T1 and above data rates.

2. Refer to Section G.8.2 for definition and how to measure.

C.2.1.5 Synchronous Optical Network Service

C.2.1.5.1 Service Description

Synchronous Optical Network Service (SONETS) is the U.S. standard for fiber optic synchronous transmission rates from 51.84 Mbps to beyond 40 Gbps while Synchronous Digital Hierarchy (SDH) is the International Telecommunications Union version, which begins at 155 Mbps. SONET transport is highly reliable and provides proactive performance monitoring that prevents single and multiple failures and further enables self-healing functions and robust network management.

C.2.1.5.1.1 Functional Definition

SONETS supports a wide range of digital signals with different capacities, and its interworking capability enables seamless communications between devices that support dissimilar protocols such as IP, Frame Relay, and ATM.

C.2.1.5.1.2 Standards

SONETS Service shall comply with the following standards unless marked optional:

1. Telcordia Technologies:
   a) (Optional) GR-1031 OTGR Section 15.6: Operations Interfaces Using OSI Tools: Test Access Management(10/97)
   b) (Optional) GR-1042 Generic Requirements for Operations Interfaces Using OSI Tools - Information Model Overview: Synchronous Optical Network (SONET) Transport Information Model (12/98)
   c) (Optional) GR-1042-IMD Generic Requirements for Operations Interfaces Using OSI Tools - Information Model Details: Synchronous Optical Network (SONET) Transport Information Model (12/98)
   d) (Optional) GR-1110 Broadband Switching System (BSS) Generic Requirements (12/00)
   e) GR-1209 Generic Requirements for Passive Optical Components (03/01)

f) GR-1230 SONET Bi-Directional Line-Switched Ring Equipment Generic Criteria (12/98)
g) GR-1250 Generic Requirements for Synchronous Optical Network (SONET) File Transfer (12/99)
h) (Optional) GR-1345 Framework Generic Requirements for Element Manager (EM) Applications for SONET Subnetworks (12/00)
i) GR-1365 SONET Private Line Service Interface Generic Criteria for End Users (12/94)
j) GR-1374 SONET Inter-Carrier Interface Physical Layer Generic Criteria For Carriers (12/94)
k) GR-1400 SONET Dual-Fed Unidirectional Path Switched Ring (UPSR) Equipment Generic Criteria (01/99)
l) GR-199 OTGR Section 12.2: Operations Application Messages - Memory Administration Messages (08/02)
m) GR-253 Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria (09/00)
n) (Optional) GR-2837 ATM Virtual Path Ring Functionality in SONET - Generic Criteria (02/98)
o) (Optional) GR-2842 ATM Service Access Multiplexer Generic Requirements (11/96)
p) (Optional) GR-2875 Generic Requirements for Digital Interface Systems (05/96)
q) (Optional) GR-2891 SONET ATM Virtual Path Digital Cross-Connect Systems - Generic Criteria (12/98)
r) (Optional) GR-2899 Generic Criteria for SONET Two-Channel (1310/1550-NM) Wavelength Division Multiplexed Systems (09/95)
s) (Optional) GR-2900 SONET Asymmetric Multiples Functional Criteria (09/95)
t) GR-2918 DWDM Network Transport Systems with Digital Tributaries for Use in Metropolitan Area Applications: Common Generic Criteria (01/03)
u) GR-2950 Information Model for SONET Digital Cross-Connect Systems (DCSS) (02/99)
v) (Optional) GR-2954 Transport Performance Management Based on the TMN Architecture (12/97)
w) (Optional) GR-2955 Generic Requirements for Hybrid SONET/ATM Element Management Systems (EMSS) (11/98)
x) GR-2979 Generic Requirements for Optical Add-Drop Multiplexers (OADMs) and Optical Terminal Multiplexers (OTMs) (12/01)

y) (Optional) GR-2980 Generic Criteria for ATM Layer Protection Switching Mechanism (12/98)
z) GR-2996 Generic Criteria for SONET Digital Cross-Connect Systems (01/99)
å) (Optional) GR-3000 Generic Requirements for SONET Element Management Systems (EMSs) (11/99)GR-3001 Generic Requirements for SONET Network Management Systems (NMS's) (12/99)
ä) (Optional) GR-3004 Generic Requirements for the Operations Interface Between Hybrid SONET/ATM Element Management Systems and Network Management Systems (02/99)
ö) GR-3008 OTGR Section 6.9: Network Maintenance: Access and Testing - SONET STS-1 and SUB-STS-1 TSC/RTU and DTAU Functional Requirements (12/98)
aa) GR-303 Integrated Digital Loop Carrier System Generic Requirements, Objectives, and Interface (12/00)
bb) (Optional) GR-3101 Generic Requirements for Asynchronous Transfer Mode (ATM) Element Management Systems (EMSs) (08/00)
cc) (Optional) GR-3102 Generic Requirements for Asynchronous Transfer Mode (ATM) Network Management Systems (10/00)
dd) (Optional) GR-376 Generic Operations Interfaces Using OSI Tools: Network Data Collection (12/98)
ee) GR-436 Digital Network Synchronization Plan (06/94)
ff) GR-496 SONET Add-Drop Multiplexer (SONET ADM) Generic Criteria (12/98)
gg) GR-499 Transport Systems Generic Requirements (TSGR): Common Requirements (12/98)
hh) GR-782 SONET Digital Switch Trunk Interface Criteria (06/00)
ii) (Optional) GR-826 OTGR Section 10.2: User Interface Generic Requirements For Supporting Network Element Operations (06/94)
jj) GR-834 Network Maintenance: Access and Testing Messages (06/00)
kk) (Optional) GR-836 Generic Operations Interfaces Using OSI Tools: Information Model Overview: Transport Configuration and Surveillance For Network Elements

2. ANSI Standards:

a) ANSI T1.105: SONET - Basic Description including Multiplex Structure, Rates and Formats
b) ANSI T1.105.01: SONET - Automatic Protection Switching
c) ANSI T1.105.02: SONET - Payload Mappings

d) ANSI T1.105.03: SONET - Jitter at Network Interfaces
e) ANSI T1.105.03a: SONET - Jitter at Network Interfaces - DS1 Supplement
f) ANSI T1.105.03b: SONET - Jitter at Network Interfaces - DS3 Wander Supplement
g) ANSI T1.105.04: SONET - Data Communication Channel Protocol and Architectures
h) ANSI T1.105.05: SONET - Tandem Connections Maintenance
i) ANSI T1.105.06: SONET - Physical Layer Specifications
j) ANSI T1.105.07: SONET - Sub-STS-1 Interface Rates and Formats Specification
k) ANSI T1.105.09: SONET - Network Element Timing and Synchronization
l) ANSI T1.119: SONET - Operations, Administration, Maintenance, and Provisioning (OAM&P) – Communications
m) ANSI T1.119.01: SONET: OAM&P Communications Protection Switching Fragment

3. ITU-T Standards:

a) Physical Interfaces:
   i. G.703 (10/98)
   ii. G.957 (06/99)
   iii. G.692 (10/98)
   iv. K.20 (05/98)
   v. G.691 (04/00)
b) Network Architecture:
   i. G.805 (11/95), (03/00)
   ii. G.803 (06/97), (03/00)
   iii. I.322 (02/99)
c) Structures & Mappings:
   i. G.704 (10/98)
   ii. G.707 (10/00) - Amendment 1
   iii. G.7041 (10/01) Generic Framing Procedure
   iv. G.7042 (10/01) LCAS
   v. G.708 (10/98)
   vi. G.832 (10/98)
d) Equipment Functional Characteristics:
   i. G.664 (06/99)

ii. G.781 (06/99)
iii. G.783 (10/00)
iv. G.958 (01/94)
v. G.705 (04/00)
vi. G.806 (04/0)

e) Laser Safety:
   i. G.664 (06/99)

f) Transmission Protection:
   i. G.841 (10/98), (08/02)
   ii. G.842 (04/97)
   iii. G.808.1 (2003)
   iv. M.2102 (03/00)

g) Equipment Protection:
   i. M.3100 Amendment

h) Equipment Management:
   i. G.784 (06/99)

i) Information Model:
   i. G.773 (03/93)
   ii. G.774 (09/92), (11/96), (04/00)
   iii. G.774.01 (11/94), (11/96), (04/00)
   iv. G.774.02 (11/94), (11/96), (04/00)
   v. G.774.03 (11/94), (11/96), (04/00)
   vi. G.774.04 (07/95), (11/96), (04/00)
   vii. G.774.05 (07/95), (11/96), (04/00)
   viii. G.774.06 (04/00)
   ix. G.774.07 (11/96), (04/00)
   x. G.774.08 (04/00)
   xi. G.774.09 (04/00)
   xii. G.774.10 (04/00)

j) Network Management:
   i. G.831 (08/96), (03/97)
   ii. T.50 (09/92)
   iii. G.85x.y (11/96)

k) Error Performance (network level view):
   i. G.826 (02/99)

ii. G.827 (02/00)
iii. G.827.1 (11/00)
iv. G.828 (02/00)
v. G.829 (02/00)
vi. M.2101 (02/00)
vii. M.2101.1 (04/97)
viii. M.2102 (02/00)
ix. M.2110 (04/97)
x. M.2120 (04/97), (02/00)
xi. M.2130 (02/00
xii. M.2140 (02/00)

l) Error Performance (equipment level view):
i. G.783 (10/00)
ii. G.784 (06/99)

m) Jitter and Wander Performance:
i. G.813 (08/96)
ii. G.822 (1988)
iii. G.823 (03/93), (03/00)
iv. G.824 (03/93), (03/00)
v. G.825 (03/93), (02/99)
vi. G.783 (10/00), (04/97), (03/99), (06/98)

n) Leased Lines:
i. M.13sdh (02/00)

o) Synchronization (Clocks and Network Architecture:
i. G.803 (06/97), (02/99)
ii. G.810 (08/96)
iii. G.811 (09/97)
iv. G.812 (06/98)
v. G.813 (08/96)

p) Test Signals:
i. O.150
ii. O.181

4. Institute of Electrical and Electronics Engineers, Inc. (IEEE):

a) IEEE 802.3, 1Gbps LAN PHY, 10Gbps LAN PHY, 10Gbps WAN PHY

b) (Optional) IEEE 802.3ae, 10Gbit Ethernet
c) 802.17, Resilient Packet Rings (RPR) – in progress
d) 802.1ah, Ethernet First Mile – in progress

5. Optical Internetworking Forum (OIF):
   a) User to Network Interface version 1.0, OIF-UNI-01.0
6. All new versions, amendments, and modifications to the above documents and standards

C.2.1.5.1.3 Connectivity

SONETS services shall connect to and interoperate with:

1. Government-specified terminations (e.g., SDP-to-SDP, POP-to-POP)
2. All other networks including other EIS contractors' networks where industry standards are used

C.2.1.5.1.4 Technical Capabilities

The following SONETS capabilities are mandatory unless marked optional:

1. Geographical Coverage. The contractor shall comply with the following requirements:
   a) (Optional) The contractor shall support OCONUS and Non-Domestic SONETS
   b) The contractor shall support Continental US (CONUS) Domestic SONETS
   c) The contractor shall support SONETS in the Metro area
2. (Optional) Gateway functionality (SONET to SDH and SDH to SONET conversion) as needed by agency.
3. The contractor shall support one or more of the following Network Topologies:
   a) Linear topologies such as Point-to-Point
   b) Ring topology
   c) Mesh topology
4. The contractor shall support one or more of the following protection methods:
   a) On the Tributary Side the contractor shall support:
      i. Automatic Protection Switching (APS) 1:N, where N ≤ 14
      ii. APS 1+1
      iii. Unprotected

b) On the Network Side the contractor shall support:
   i. Unprotected
   ii. Mesh Protection
   iii. Unidirectional Path Switched Ring (UPSR)
   iv. Bidirectional Line Switched Ring (BLSR)
   v. (Optional) Bidirectional Path Switched Ring (BPSR) or equivalent
   vi. 1+1

5. Transmux Capability (interconnects high bandwidth interface at one agency location to lower bandwidth interface at another agency location):
   a) (Optional) DS3/STS1 transmuxed to DS1 shall be supported
   b) OC3 transmuxed to DS3/STS1 shall be supported
   c) OC12 transmuxed to OC3/DS3/STS1 shall be supported
   d) OC48 transmuxed to OC12/OC3/DS3/STS1 shall be supported
   e) (Optional) OC192 transmuxed to OC48/OC12/OC3/DS3/STS1 shall be supported
6. (Optional) The following concatenation methods shall be included in SONETS:
   a) Standard Concatenation. SONET specifications in GR-253 include standard concatenation, which allows OC-N signals to be grouped in multiples of 3 STS-1s and treated as single entities. The following standard concatenated rates shall be supported:
      i. STS-12c shall be supported
      ii. STS-48c shall be supported
      iii. (Optional) STS-192c shall be supported
      iv. (Optional) STS-768c shall be supported
   b) Virtual Concatenation. The following standard rates shall be available for agency procurement: (Optional)
      i. VT-1.5-7v for 10 Mbps Ethernet Connections shall be supported
      ii. VT-2.0-5v for 10 Mbps Ethernet Connections shall be supported
      iii. STS-1-2v for 100 Mbps Fast Ethernet Connections shall be supported
      iv. STS-1-21v for 1Gbps Ethernet Connections shall be supported
      v. STS-3c-7v for 1Gbps Ethernet Connections shall be supported
   c) The contractor shall support the following:
      i. High order concatenation – shall support STS-1/3c-*X*v SPE, *X* = 1 up to 256 rates/entities

ii. Low order concatenation – shall support X VTn SPEs (n=1.5, 2, 3, 6) rates/entities

7. Performance Monitoring: The contractor shall support the Performance Monitoring parameters specified by GR-253. Monitoring of parameters shall be for each individual minute and recorded in registers of 15 minutes. The last eight 15-minute registers shall be archived and made accessible to the agency. The contractor shall store all measurements for the past 24 hours in a register. The following parameters shall be monitored, and measured:

   a) Errored Seconds. An Errored Second is any one-second interval containing at least one error. Errored Seconds shall be counted as 1-second intervals containing at least 1 error. The contractor shall measure performance based on percent of error seconds, which is calculated as 100 times the ratio of error seconds to total seconds in the available time during a fixed measurement period (24 hours). For all EIS users, the percentage of Errored Seconds shall be less than 0.25% during the measurement period. It is AQL to observe Errored Seconds during 1.8 minutes per month.

   b) Severely Errored Seconds (SES). A SES is 1-second period with a bit error rate per second of 10^{-3} or worse for DS-1 and DS-3 signals. SES for STS-n signals, is 1-second period that contains 30 percent or greater errored blocks or at least one severely disturbed period. A severely disturbed period occurs when all contiguous blocks are affected by a high bit error density over a period of 1 millisecond. The contractor shall measure performance based on percent of SES, which is calculated as 100 times the ratio of SES to total seconds in available time during a fixed measurement period (24 hours). For all EIS users, the percentage of SES shall be less than 0.035% during the measurement period. It is AQL to observe SES during 15.12 seconds per month.

8. Synchronization and Timing Methods. The contractor shall support the following:

   a) External Timing

   b) Line Timing

9. Reserved

10. (Optional) Next Generation SONET shall be supported.

11. The contractor's network shall support all of the following:

    i. Generic Framing Procedure, shall include:

       1. Frame Mapped Generic Framing Procedure
       2. Transparent Generic Framing Procedure

ii. Link Adjustment Capacity Scheme (LCAS) shall be supported to provide Virtual Concatenation as defined by ANSI T1.105 and G.707

iii. (Optional) Virtual Concatenation shall be supported.

12. (Optional) Data Communications Channel (DCC) – The contractor shall provide the agency with the ability to establish communication between its edge devices.

13. (Optional) Integrated Control Plane (i.e. ASON based, GMPLS) – Support of an integrated, intelligent control plane in order to speed up activation service times, provide control to agencies to the contracted infrastructure and achieve inter- and intra-contractor interoperability when required.

C.2.1.5.2 Features

The following SONETS Service features are mandatory unless marked optional:

Service Features ID Number	Name of Feature	Description
1 (optional)	Channelization	The contractor shall support SONET interfaces to the CPE to seamlessly interface with the contractor's SONET network for data transport. The following channelized arrangements shall be supported as a minimum: 1. STS-1 payload with VT1.5, VT2 2. STS-1, STS-1 payload, VT1.5, VT2, STS-3c 3. VC-11(DS1), VC-12 (E1), VC-3 (DS3, E3, other) 4. VC-4, VC-3, VC-11, VC-12 5. Down to STS-1 (E3, other) 6. STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4
2 (Optional)	DS1 Rate Synchronization Service	The contractor shall provide the agency with this feature to allow agency's Stratum 2 or Stratum 3 clocks at its locations to synchronize to a Stratum 1 clock at the contractor's location. The DS1 to be used for synchronization shall be delivered through the following methods: 1. External Timing

Service Features ID Number	Name of Feature	Description
3	SONET Performance	All SONET services contracted by the agencies shall comply with the following performance indicators and with the Performance Metrics included in Section C.2.1.5.4: 1. Jitter -- as specified in GR-253 - Jitter measurement is performed over a 60-second interval with band pass filters having frequencies cut off at 10 KHz and 4 KHz, a fall of 20db/decade, and a low-pass cut off frequency of at least 80 KHz. The contractor shall ensure these specifications are met at the SDPs. 2. Restoration Time -- as specified by GR-253 for Automatic Protection Switching and by GR-1230, Section 6.1.1, re-routing of the traffic shall be performed to restore the SONETS (over redundant path) before the failure is repaired. The contractor shall reconfigure affected services for Rings < 1200 KM as follows: a) For Routine Users, in less than 100 ms, when preemption of extra traffic is required. b) For Critical Users, in less than 60 ms including detection time (10ms).
4	Equipment Protection – Network Side	The contractor shall provide protection to the client interfaces at the SDP, where the protection channel is bridged to the failed working channel.
5	Framing for Electrical Interfaces	The following framing formats for electrical interfaces shall be supported: 1. (Optional) M-frame with M23 Multiplexing format. 2. M-frame with C-parity. 3. (Optional) Super Frame (SF) Format. 4. (Optional) Bipolar Alternate Mark Inversion. 5. Binary, 8 zero substitution line code.

Service Features ID Number	Name of Feature	Description
		6. (Optional) Non-ANSI SF. 7. ANSI Extended Superframe (ESF) (ANSI T1403, 1995). 8. (Optional) Non-ASNI ESF (AT&T PUB 54016).
6	Geographic Diverse Protection	The feature shall ensure a minimum separation of 25 feet between the diverse circuits end-to-end. In addition, the contractor shall ensure that the diverse circuits are specifically flagged to prevent disconnection during network grooming activity.
7	Local and Remote Node Multiplexing	This feature shall enable the multiplexing of different low-speed circuits onto a high-speed SONET signal, such as SONET OC3 and OC12.

C.2.1.5.3 Interfaces

The UNIs at the SDP are mandatory unless marked optional.

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling/Protocol Type/Granularity
1	Optical	IEEE 802.3z	1310 nm	1.25Gbps	Gigabit Ethernet
2	Optical	IEEE 802.3z	850 nm	1.25Gbps	Gigabit Ethernet
3	Optical	IEEE 802.3	1310 nm	125 Mbps	Fast Ethernet
4	Optical	GR-253, ITU-T G.707	1310 nm	155 Mbps	SONET or SDH
5	Optical	GR-253, ITU-G.707	1310 nm	155 Mbps	SONET or SDH Concatenated
6	Optical	GR-253, ITU-G.707	1310 nm	622 Mbps	SONET or SDH
7	Optical	GR-253, ITU-G.707	1310 nm	622 Mbps	SONET or SDH Concatenated
8	Optical	GR-253, ITU-T G.707	1310 nm	622 Mbps	SONET Channelized
9 (Optional)	Optical	GR-253	1310 nm	155 Mbps	ATM over SONET
10 (Optional)	Optical	GR-253	1310 nm	622 Mbps	ATM over SONET
11	Optical	GR-253, ITU-T G.707	1310 nm	2.5Gpbs	SONET or SDH

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling/Protocol Type/Granularity
12	Optical	GR-253, ITU-T G.707	1310 nm	2.5Gbps	SONET or SDH Concatenated
13 (Optional)	Optical	GR-253, ITU-T G.707	1310 nm	10Gbps	SONET or SDH
14	Electrical	ANSI T1	N/A	1.544 Kbps	DS1
15	Electrical	ANSI T1	N/A	45 Mbps	DS3
16	Electrical	ANSI T1	N/A	45 Mbps	STS-1
17	Electrical	ANSI T1	N/A	DS1	DS0, Nx64 Kbps
18	Electrical	ANSI T1	N/A	DS3	DS3, Nx1.544Mbps, DS1
19	Electrical	ANSI T1	N/A	E1	Nx64 Kbps
20	Electrical	ANSI T1	N/A	E3	E1, Nx64 Kbps, DS0
21 (Optional)	Optical	GR-253, ANSI T1.105	1300 nm	OC-1	SONET STS-1 payload, VT1.5, VT2
22 (Optional)	Optical	GR-253, ANSI T1.105	1300 nm	OC-3 155 Mbps	SONET STS-1, STS-1 payload, VT1.5, VT2
23	Optical	GR-253, ANSI T1.105	1300 nm	OC-3c 155 Mbps	SONET STS-3c
24	Optical	G.707	1300 nm	STM-1 155 Mbps	SDH VC-11(DS1), VC-12 (E1), VC-3 (DS3, E3, other)
25	Optical	G.707	1300 nm	STM-1c 155 Mbps	SDH VC-4, VC-3, VC-11, VC-12
26 (Optional)	Optical	GR-253, ANSI T1.105	1300 nm	OC-12 622 Mbps	SONET Down to VT1.5 (DS1), VT2 (E1), STS-1 (DS3, E3, other), STS-3c
27	Optical	GR-253, ANSI T1.105	1300 nm	OC-12c 622 Mbps	SONET STS-12c
28	Optical	ITU-T G.707	1300 nm	STM-4	SDH STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4
29	Optical	ITU- G.707	1300 nm	STM-4c	VC-4-4c
30 (Optional)	Optical	OIF- VSR4-01.0	850 nm	OC-192	VSR4-01 OC-192 (12 fibers)
31 (Optional)	Optical	OIF-VSR4-03.0	1310 nm	OC-192	VSR4-02 OC-192 (1 fiber)

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling/Protocol Type/Granularity
32 (Optional)	Optical	OIF-VSR4-03.0	850 nm	OC-192	VSR4-03 OC-192 (4 fibers)
33 (Optional)	Optical	OIF-VSR4-04.0	850 nm	OC-192	VSR4-04 OC-192 (1 fiber)
34 (Optional)	Optical	OIF-VSR4-05.0	1310 nm	OC-192	VSR4-05 OC-192
35 (Optional)	Optical	OIF-VSR5-01	850 nm	OC-768	VSR5-01 OC-768
36	Electrical	GR-253, ANSI T1.105	850 nm	STS-1/EC-1 51.84 Mbps	SONET/STS-1, VT1.5 mapping
37 (Optional)	Optical	GR-253	1550 nm	2.5 Gbps	SONET or SDH
38 (Optional)	Optical	GR-253	1550 nm	10 Gbps	SONET or SDH

C.2.1.5.4 Performance

The contractor shall support In-Service Monitoring (ISM) at the SONET Layer and shall not rely on performance observed and measured at higher layers of the network.

The performance levels and AQL of KPIs for SONET Service are mandatory unless marked optional.

Key Performance Indicators	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(SONETS) (SDP-to-SDP)	Routine	99.8%	≥ 99.8%	In Service Monitoring See Note 1
	Critical	99.999%	≥ 99.999%	
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. SONETS availability shall be measured in-service and on an end-to-end basis. COT (HR) shall be calculated based on Errored Seconds and/or SES as defined by GR-253, G.826 through G.829 and shall be expressed in hours. Availability is computed by the standard formula:

$$Av(SONETS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

.

C.2.1.6 Dark Fiber Service

C.2.1.6.1 Service Description

Dark fiber is optical fiber infrastructure (cabling and repeaters) in which the light is provided by the customer rather than the carrier. The simplest Dark Fiber Service (DFS) is a point-to-point connection between two locations. Other configurations enable agencies to interconnect any number of selected locations.

C.2.1.6.1.1 Functional Definition

DFS is acquired as a facility which allows the agency the unconditional right to use a fiber route, which provides capacity such as a fiber pair in a fiber-optic cable or the entire fiber-optic cable. Agencies which acquire dark fiber may either provide their own optronics equipment or lease it from the contractor. Agencies which prefer not to design, implement, and manage their own optical networks can use Managed Network Service (MNS) as a Managed Dark Fiber Service to design, implement, and manage optical networks to meet their unique mission requirements.

C.2.1.6.1.2 Standards

DFS shall comply with the following standards:

1. Electronic Industry Alliance/Telecommunications Industry Association (EIA/TIA):
   a) EIA/TIA-559, Single Mode Fiber Optic System Transmission Design.
   b) Optical Fiber System Test Procedures (OFSTPs) including:
      i. OFSTP-2, Effective Transmitter Output Power Coupled into Single Mode Fiber Optic Cable
      ii. OFSTP-3, Fiber Optic Terminal Receiver Sensitivity and Maximum Receiver Input
      iii. OFSTP-7, Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant
      iv. OFSTP-14, Measurement of Optical Power Loss of Installed Multi-Mode Fiber Cable Plant
      v. OFSTP-10, Measurement of Dispersion Power Penalty in Single Mode Systems
      vi. OFSTP-11, Measurement of Single Reflection Power Penalty for Fiber Optic Terminal Equipment
2. Telcordia Standards:

a) GR-20-CORE, Generic Requirements for Optical Fiber and Optical Fiber Cable
b) GR-63-CORE, Network Equipment-Building System (NEBS), Generic Equipment Requirements
c) GR-253-CORE, Synchronous Optical Network (SONET) Transport Systems: Common Criteria Physical Layer
d) GR-326-CORE, Generic Requirements for Single Mode Connectors and Jumper Assemblies

3. American National Standards Institute (ANSI):
   a) ANSI Z136.2-1998, American National Standard for the Safe Use of Optical Fiber Communications Systems Utilizing Laser Diode and LED Sources
4. International Electrotechnical Commission (IEC):
   a) IEC 60825-1,Safety of Laser Products, Part 1: Equipment Classification, Requirements and User's Guide, Consolidated Edition – International Restrictions
   b) IEC 60825-2, Safety of Laser Products, Part 2: Safety of Optical Fiber Communications Systems (OFCS) – International Restrictions.
5. Code of Federal Regulations (CFR):
   a) 21 CFR 1040, Performance Standard for Laser Products
6. International Telecommunications Union (ITU-T):
   a) ITU-T G.655 (10/2000)
   b) ITU-T G.652 (10/2000)
   c) ITU-T G.694.1
   d) ITU-T K.25 (02/2000)
   e) ITU-T L.35 (10/1998)
7. Regulations and Permits – The contractor shall be responsible for all permits, easements, and rights of way, to include Host Nation agreements/approvals. The contractor shall be responsible for complying with local government regulations. If obstacles are found during the process that will affect agency's schedule negatively, the contractor shall coordinate solutions with the government.
8. All new versions, amendments, and modifications to the above documents and standards.

C.2.1.6.1.3 Connectivity

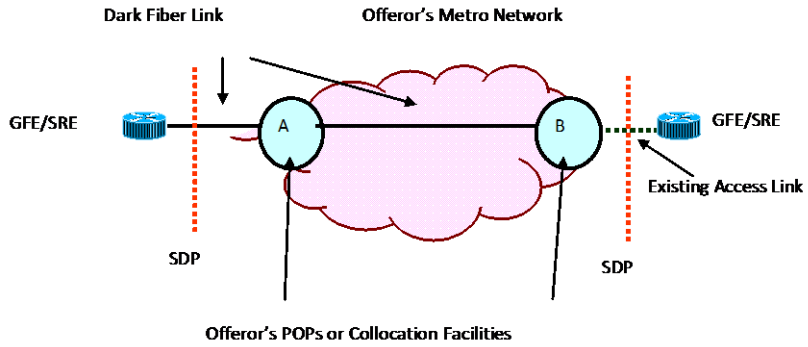
DFS shall connect to and interoperate with:

1. Inter-agency or intra-agency LANs within the same vicinity. This service shall enable an agency to interconnect via inter-agency or intra-agency LAN to selected locations situated within the same metro area (i.e., city). Examples of supported configurations are outlined in Section C.2.1.6.1.4 #2.
2. The contractor's Long Haul or Metro networks. This service shall enable an agency to connect its locations(s) to the nearest contractor's wire center, LEC wire center, Hut, IXC POP, or CLEC collocation facility as applicable.
3. Redundant paths to support agency's transport infrastructure, thereby enhancing service reliability.
4. The contractor shall terminate fiber(s) in the existing Fiber Distribution Panel (FDP) or the FDP specified by the agency using connectors specified by industry's standards for:
   a) Multi-tenant buildings
   b) Single tenant buildings

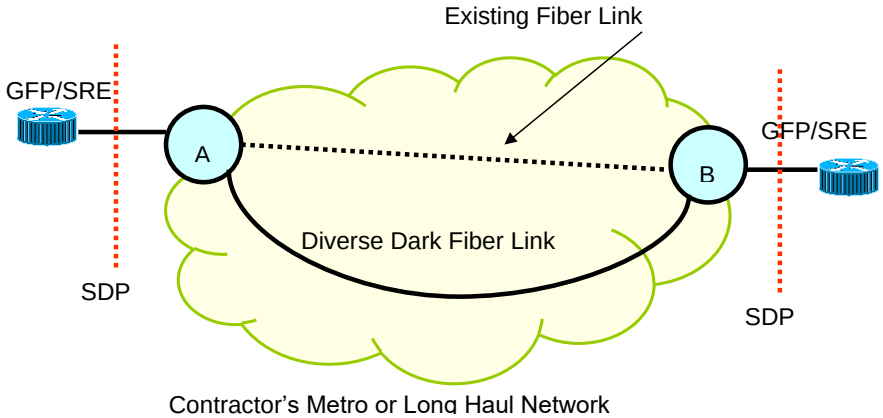
C.2.1.6.1.4 Technical Capabilities

The following DFS capabilities are mandatory unless marked optional:

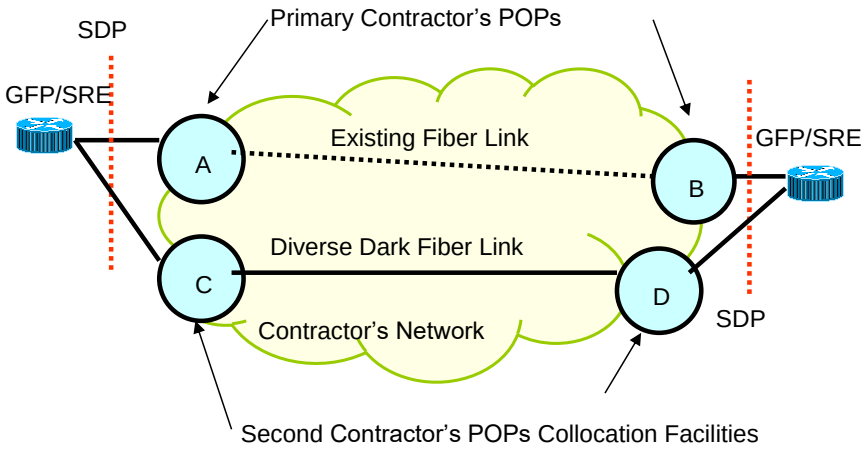
1. Geographical Coverage. The contractor shall specify the coverage of its DFS in the following regions when required as part of a TO:
   a) CONUS
   b) (Optional) Non-domestic
   c) (Optional) OCONUS
2. Configuration Alternatives. The contractor shall support the network topologies outlined as follows:
   a) Point-to-point. This configuration connects any two points in the contractor's network. The figure below depicts two agency locations in a metro area connected by a dark fiber link from POP to POP.



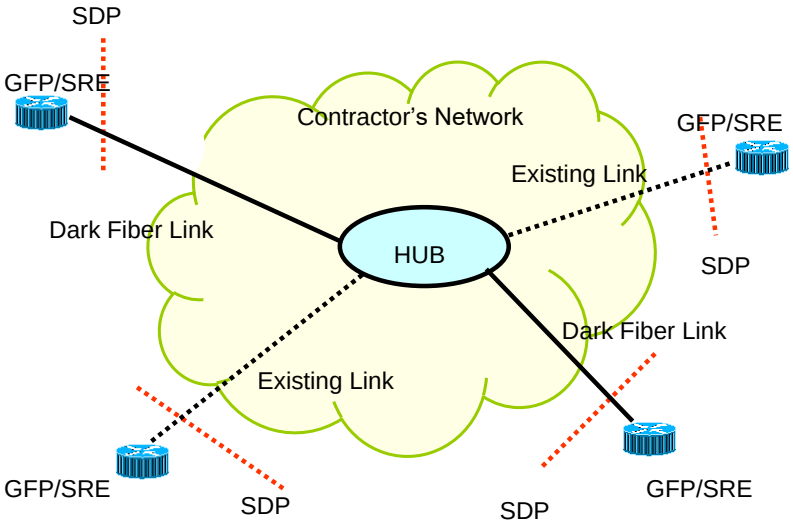
b) Route Diversity Ring/Single Drops. This configuration is possible when the terminating equipment provides equipment and/or line protection schemes. The figure below shows that two diverse paths are available on the network to prevent service interruptions if either fiber path is damaged.



c) Route Diversity Ring/Dual Drops. This configuration is possible when two diverse paths are available end-to-end to prevent service interruptions caused by a failure in either path. The diverse path can be purchased from the same contractor and delivered to two different POPs or from a second contractor. The figure below shows that an agency has built an alternate route for protection (path C-D) using a second contractor's POPs or collocation facilities where the agency has placed its optronics.



d) Star Configuration. This configuration allows an agency to have a single location that functions as a hub that provides connectivity to other agency locations. The figure below depicts a point-to-point configuration.



Hybrid Configuration. The preceding configurations can be combined to yield a custom-tailored solution.

1. Fiber Service Delivery Point (FSDP). The contractor shall support the SDP at either the fiber patch panel where the fibers terminate at a government location or the collocation facility where the agency has installed its optronics, as required by the agency. The contractor shall meet the following conditions when delivering DFS to an agency:
    a) Optical Fiber. The fiber shall meet the standards specified in Section C.2.1.6.1.2. The contractor shall provide the number of fiber strands to be delivered at the FSDP as specified by the agency.
2. Ducting. The contractor shall provide the number of ducts between connecting locations and the number of fiber strands running in each duct as specified by the agency.
3. (Optional) Future Growth. The contractor shall include an additional duct running in parallel to the working duct(s) to provide room for anticipated growth.
4. Channel Count:
    a) Deployed fibers shall be capable of supporting a minimum of 80 DWDM wavelengths or user data with spacing as specified in ITU-T G.694.1.
    b) Deployed fibers shall be capable of operating in the "C", ”S” and “L” bands.
5. Gateways. The contractor shall provide the ability to add and drop traffic via gateway locations (nodes A, B, C, and D in the Configuration Options diagrams above are examples of gateways). The contractor shall fulfill the following requirements and provide updates on improvements or expansions throughout the life of the contract:
    a) Gateway locations shall be equipped with backup power capability and shall operate for at least 8 hours without interruption
    b) Lock cabinet spaces shall be provided
    c) 24x7 access to the gateway locations shall be provided to authorized personnel
    d) Gateway locations shall be equipped with surveillance and highly secured systems
    e) The contractor shall indicate if gateway expansion is possible
    f) The contractor shall indicate if gateway locations are monitored remotely
    g) Environmental monitoring shall be supported
6. Service Components. DFS service components shall include the following:

a) Trunks. Trunks are main fiber cables that may carry hundreds of fiber strands, which may be shared and owned by a variety of contractors, government agencies, universities, etc.
b) Laterals. Laterals are fiber cables from the agency's premises to the nearest splice point on the cable trunk. Their length may vary from a few meters to several kilometers.
c) Building Entrances. Facilities within the agency's premises for the termination of fibers, i.e., fiber panel terminations.

C.2.1.6.2 Features

The following DFS features are mandatory unless marked optional.

ID Number	Name of Feature	Description
1	Colocation Service	The contractor shall provide the ability to add/drop traffic (gateways) and to regenerate and amplify traffic where needed.
2 (Optional)	Duct	The contractor shall support the number of ducts (conduits) as specified by the agency that shall be included in the service.
3 (Optional)	Dark Fiber Local Loop	The contractor shall provide dark fiber connection between the agency's location and the contractor's wire center or outside plant (hut or regeneration location).
4 (Optional)	Diverse Route Single Drop	The contractor shall ensure that two diverse paths are available on the network to prevent service interruptions if a fiber on either of two paths is damaged. A Single Add/Drop location/network element shall be used in this arrangement with automatic protection switching capabilities.
5 (Optional)	Diverse Route Dual Drop	The contractor shall provide two diverse paths end-to-end to prevent service interruptions caused by a failure either in the contractor's network or at the drop's path. A second contractor shall provide the diverse route should the agency requires full diversity for protection unless the working link provider is able to do so.
6 (Optional)	Inter-city Connectivity	The contractor shall support a dark fiber connection between agency's locations in metro areas in the Continental US as well as outside the Continental US.

ID Number	Name of Feature	Description
7 (Optional)	Multiple Duct	The contractor shall be able to upgrade to multiple ducts (conduits).
8	Splicing	The contractor shall support joining two or more lengths of optical fiber cables by way of either fusion or mechanical splicing.
9	Off-net laterals	The contractor shall provide fiber cables from the agency's premises to the nearest splice point on the cable trunk. They shall be funded by the agency and their length may vary from a few meters to several kilometers.

C.2.1.6.3 Interfaces

The interfaces for this service are the fiber terminations at the FSDP. The contractor shall identify the fiber connectors that are supported.

C.2.1.6.4 Performance Metrics

The performance levels and AQL of KPIs for DFS are mandatory unless marked optional:

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Attenuation Coefficient SMF (1550 nm)	Routine	0.25 dB/km	≤ 0.25 dB/km at all times	See Note 1
Attenuation Coefficient SMF (1310 nm)	Routine	0.35 dB/km	≤ 0.35 dB/km at all times	
Attenuation Coefficient MMF 850 nm (50/125 µm)	Routine	2.35 dB/km	≤ 2.35 dB/km at all times	

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Attenuation Coefficient MMF 1300 nm (50/125 µm)	Routine	0.35 dB/km	≤ 0.35 dB/km at all times	
Polarization Mode Dispersion (PMD) at 1550 nm (Inter-City Networks)	Routine	May be specified in TO	May be specified in TO	See Note 2
Polarization Mode Dispersion (PMD) (Intra-City Networks)	Routine	May be specified in TO	May be specified in TO	
Chromatic Dispersion at 1550nm	Routine	May be specified in TO	May be specified in TO	See Note 3
Reflectance Events (all events)	Routine	Less than 40 dB	≤ 40 dB at all times	See Note 4
Connectors Loss SMF	Routine	0.1 to 0.2 dB	≤ 0.2 dB at all times	
Fusion Splicing Loss SMF	Routine	0.05 dB	≤ 0.05 dB at all times	
End-to-End Attenuation	See Note 5			
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 6
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Attenuation coefficient is the attenuation per unit length with a maximum value at one or more wavelengths. In this case, wavelengths are from 1310nm to 1550nm.
2. Polarization Mode Dispersion (PMD) is the term that describes the relationship between polarization and group delay.
3. Chromatic dispersion measurements characterize how the velocity of propagation in fiber or components changes with wavelength.
4. Reflection measurements are done using an optical time-domain reflectometer (OTDR).
5. End-to-End Attenuation
    a. On Single Mode Fibers (SMF), end-to-end attenuation measurements shall be tested in both directions of transmission at the 1310 nm and 1550 nm wavelengths using an industry-accepted laser source and power meter.
    b. On Multi Mode Fibers (MMF), end-to-end attenuation measurements shall be tested in both directions of transmission at the 850 nm and 1300 nm wavelengths.
    c. Loss measurements shall be taken from both ends at applicable wavelengths as in subparagraphs i and ii above, and in compliance with OFSTP-7 and OFSTP-14 or EIA/TIA-568 B as applicable.
    d. OTDR measurements shall be performed for each fiber for length, transmission anomalies, and end-to-end attenuation.
    e. A written report shall be issued and delivered to the OCO for each cable, and OTDR traces and other measurements shall be included for each fiber and provided periodically as specified in the TO.
6. See Section G.8.2 for definition and how to measure.

C.2.1.7 Internet Protocol Service

The government uses Internet Protocol Service (IPS) to support a wide range of connectivity requirements that enable government users to access the Internet, government-wide intranets, and extranets. IPS will use the TCP/IP protocol suite to interconnect GFP/SRE with other government networks and the public Internet Service Provider (ISP) networks.

C.2.1.7.1 Service Description

This section provides the IPS description.

C.2.1.7.1.1 Functional Description

IPS provides transport of Internet Protocol (IP) packets.

C.2.1.7.1.2 Standards

IPS shall comply with the following standards:

1. Internet Engineering Task Force (IETF) RFCs
2. ANSI T1
3. ITU TSS Recommendations
4. IEEE:
   a) 802.1Q
   b) 802.1P
   c) (Optional) 802.3AD
5. Metro Ethernet Forum (MEF)
6. IETF RFCs for IPv6
7. All new versions, amendments, and modifications to the above documents and standards

C.2.1.7.1.3 Connectivity

IPS shall connect:

1. Government locations, including mobile and remote users, (i.e., SDP devices such as customer routers, switches, and firewalls) to the Internet.
2. A wide range of equipment (such as notebook PCs, PDAs, etc.) via appropriate combinations of EIS services to the Internet.
3. Government locations to other networks, including those of other EIS contractors.

C.2.1.7.1.4 Technical Capabilities

The following IPS capabilities are mandatory unless marked optional:

1. The contractor shall meet applicable routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.
2. The contractor shall provide IPS ports at the peak data rates specified by the customer.

3. The contractor shall support appropriate access services (such as DSL, cable high speed access, PLS, or satellite) to connect customer SDPs to the contractor's IPS.
4. The contractor's network shall have:
   a) Established public peering arrangements from the contractor's network to the Internet.
   b) Private peering arrangements established from the contractor's network with redundant links to connect to its private peering partners.
   c) Support for the government-assigned and InterNIC-registered IP addresses and domain names.
   d) Primary and Secondary Domain Name Service (DNS) to provide an authoritative name server for the customer.
5. The contractor shall provide support for the Border Gateway Protocol (BGP) for EIS customers with registered Autonomous System (AS) numbers.
6. The contractor shall validate routing protocol information using authenticated protocols. BGP sessions shall be configured in accordance with, but not limited to, the NIST SP 800-54 recommendation that BGP sessions are protected with the MD5 signature option.

C.2.1.7.2 Features

The IPS feature is mandatory.

ID Number	Name of Feature	Description
1	Class of Service (CoS)	The contractor shall accommodate and optimize an agency's applications to enable the network to accurately and consistently allow for traffic prioritization and cost-efficiencies. The Classes of Service or prioritization levels may be categorized as: 1. Premium — for time-critical traffic such as voice and video 2. Enhanced — for business-critical traffic such as transactions 3. Standard — for non-critical traffic such as email.

C.2.1.7.3 Interfaces

These UNIs at the SDP for the provisioning of IPS are mandatory unless marked optional.

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
1 (Optional)	Cable High Speed Access	256 Kbps up to 150 Mbps (Standard DOCSIS 3.0)	Point-to-Point Protocol, IPv4/v6
2	Ethernet Interface	1. 1 Mbps up to 1 GbE (Gigabit Ethernet) 2. 10 GbE (Optional) 3. Burstable	IPv4/v6 over Ethernet
3	IP over SONET Service	1. OC-3c 2. OC-12c 3. OC-48c 4. OC-192c	IP/PPP over SONET
4	Private Line Service	1. DS0 2. T1 3. T3 4. OC-3c 5. OC-12c 6. OC-48c 7. OC-192c	IPv4/v6 over PLS
5 (Optional)	DSL Service	xDSL access at 1.5 to 8 Mbps downlink, and 384 Kbps to 1.5 Mbps uplink	Point-to-Point Protocol, IPv4/v6
6 (Optional)	FTTP	256 Kbps to 150 Mbps	Point-to-Point Protocol, IPv4/v6
7 (Optional)	Wireless Access	1. LTE 2. Satellite	Point-to-Point Protocol, IPv4/v6

C.2.1.7.4 Performance Metrics

The performance levels and AQL of KPIs for IPS are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Av(Port)	Routine	99.95%	≥ 99.95%	See Note 1
	Critical	99.995%	≥ 99.995%	
Latency (CONUS)	Routine	60 ms	≤ 60 ms	See Note 2
	Critical	50 ms	≤ 50 ms	
GOS (Data Delivery Rate)	Routine	99.9%	≥ 99.9%	See Note 3
	Critical	99.99%	≥ 99.99%	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Port availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the port is operationally available to the agency. Availability is computed by the standard formula:

$$Av(Port) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Latency is the average time for IP packets to travel across the contractor's infrastructure. The Latency metric does not apply for the DSL, Cable High Speed, Wireless, and Satellite access methods. Packet delivery and latency can be calculated using the Internet Control Message Protocol (ICMP) test, in which a series of five test packets is sent every five minutes between contractor service aggregation points (i.e., POPs). The test results are analyzed to determine packet loss vs. successful delivery and speed of delivery. The relevant standards are RFC 1242 and RFC 2285.
3. Network packet delivery is a measure of IP packets successfully sent and received across the contractor's infrastructure. The data delivery rate can be measured with the ICMP test (Data Delivery Rate %) = (100 - Packet Loss %).
4. See Section G.8.2 for the definitions and measurement guidelines.

C.2.2 Voice Service

The technical requirements for Voice Service (VS) are provided in Sections C.2.2.1 and C.2.2.2.

VS can be provided using various technologies. The services are organized as follows:

1. Internet Protocol Voice Service
2. Circuit Switched Voice Service

The contractor shall provide at least one of the VS technologies specified above as its mandatory VS solution. The contractor may propose to provide both forms of VS.

C.2.2.1 Internet Protocol Voice Service

Internet Protocol Voice Service (IPVS) provides voice communications service and telephony features to agencies using VoIP over a managed IP network.

C.2.2.1.1 Service Description

IPVS shall provide a network-based (hosted) and premises-based telephone service over the contractor-provided IP network. The contractor shall also provide a Managed LAN Service (see Section C.2.2.1.5) and Session Initiation Protocol (SIP) Trunking Service (see Section C.2.2.1.6).

C.2.2.1.1.1 Functional Definition

IPVS supports voice calls, whether initiated from on-net or off-net locations, to be connected to all on-net and off-net locations by direct dialing.

C.2.2.1.1.2 Standards

IPVS shall comply with the following standards:

1. ITU-T G.711
2. (Optional) ITU-T G.723.x, G.726, G.728, or G.729.x
3. ITU-T H.323, H.350
4. Real-Time Transport Protocol (RTP) IETF RFC 3550
5. Session Initiation Protocol (SIP) IETF RFC 3261

C.2.2.1.1.3 Connectivity

IPVS shall connect to and interoperate with wireline and wireless networks, other EIS contractor voice networks, and satellite-based voice networks, in both domestic and non-domestic locations, using interconnects to the PSTN.

C.2.2.1.1.4 Technical Capabilities

The IPVS shall include unlimited on-net to on-net and on-net to CONUS off-net calling. The IPVS shall support off-net calling to CONUS, OCONUS, and Non-Domestic locations. The contractor shall provide capabilities that enable IPVS users to establish and receive telephone calls between both on-net locations and the PSTN.

The contractor shall provide a remote access capability that, once enabled, provides users with the ability to use any landline or cell phone to make or receive phone calls as if they were making or receiving calls with VoIP phones.

The following capabilities are mandatory unless marked optional:

1. Real time transport of voice, facsimile, and TTY communications
2. Real time delivery of Automatic Number Identification (ANI) information (when provided from the originating party)
3. Interoperate with public network dial plans (e.g., North American Numbering Plan and ITU-E.164)
4. Interoperate with private network dial plans and support direct dialing
5. (Optional) Interoperate with non-commercial, agency-specific 700 numbers
6. Provide access to public directory and operator assistance services
7. Provide unique directory numbers for all on-net government locations, including support for existing government numbers.
8. Provide the capability to initiate automatic callback
9. Support 3-way calling

The contractor shall provide gateways for interoperability between the contractor's IP-based network and the PSTN, or with agency UNIs. The specific gateway will depend upon the ordering agencies UNI requirements. The gateways and functionality are described below:

1. Subscriber Gateway – The contractor shall provide interoperability for non-IP telephone devices. The contractor shall provide non-proprietary telephony station UNIs including (a) analog station and (b) ISDN BRI station interfaces.
2. PSTN Gateway – The contractor shall provide transparent access to and interwork with the domestic and non-domestic PSTNs.

The contractor shall provide the capability to support station mobility. Station mobility enables IP subscribers to dynamically move IP phones within the agency's enterprise wide network and access IP services.

The contractor's IPVS shall have the capability to traverse and successfully interoperate with agency firewalls and security layers. The contractor shall verify with the agency that the agency firewall is compatible with the contractor's service.

The contractor shall ensure that security practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized access. This includes SIP-specific gateway security for SIP firewalls, where applicable. The contractor shall ensure that security practices and policies are regularly updated and audited. The general areas of security to be addressed are:

1. Denial of service – The contractor shall provide safeguards to prevent hackers, worms, or viruses from denying legitimate users from accessing IPVS.
2. Intrusion – The contractor shall provide safeguards to mitigate attempts to illegitimately use IPVS.
3. Invasion of Privacy – The contractor shall ensure that IPVS is private and that unauthorized third parties cannot eavesdrop or intercept IPVS communication numbers, IP addresses or URLs.

The contractor shall fully comply with emergency service requirements, including 911 and E911 services, and identify the location of originating stations and route them to the appropriate Public Safety Answering Point (PSAP).

The contractor's IPVS shall comply with the Federal Communications Commission (FCC) Local Number Portability (LNP) requirements.

C.2.2.1.2 Features

The following IPVS features are mandatory unless marked optional.

ID Number	Name of Feature	Description
1	Voice Mail Box	The contractor shall offer voice mail capability that includes voice messaging transmission, reception, and storage 24x7 except for periodic scheduled maintenance. The contractor-provided voice mailbox shall meet the following minimum requirements: 1. At least sixty minutes of storage time (or 30 messages) 2. Ability to remotely access voice mail services 3. Secure access to voice mail via a password or PIN 4. Automatic notification when a message is received 5. Minimum message length of two minutes 6. Capability to record custom voice mail greetings

ID Number	Name of Feature	Description
		This capability can be administered on a station basis according to the ordering agency's needs. The contractor shall send an email with a WAVE (.wav) file attachment of each voicemail message received by users of this feature to the email address that the user designates. The contractor shall provide users the capability to add other notification devices / email addresses or to update email information and email preferences when receiving and forwarding messages through a secure user web portal.
2	Auto Attendant	Auto Attendant allows callers to be automatically transferred to an extension without the intervention of an operator. The contractor shall provide capabilities allowing callers to dial a single number for high volume call areas and to select from up to nine (9) options to be directed to various attendant positions, external phone numbers, mailboxes or to dial by name or extension at a minimum.
3	Augmented 911/E911 Service	The contractor shall appropriately populate a 911 Private Switch/Automatic Location Identification (PS/ALI) database with the government's profile which shall include all the users' telephone numbers, station locations, building location, building address, building floor, and room number during service implementation.The contractor shall provide secure remote access to the government via a client or a web browser to allow the government to maintain the government's profile on an ongoing basis (e.g., to account for moves, adds, deletions, or other changes). The contractor shall ensure these government profile updates are reflected in the PS/ALI database.

The following standard features shall be included in the basic service:

1. Caller ID
2. Conference Calling
3. Do Not Disturb
4. Call Forward – All
5. Call Park
6. Hotline
7. Call Forward – Busy
8. Call Pickup
9. Hunt Groups
10. Call Forward – Don't Answer
11. Class of Service Restriction

12. Multi-Line Appearance
13. Call Hold
14. Distinctive Ringing
15. Directory Assistance
16. Call Transfer
17. Call Waiting
18. Speed Dial
19. Call Number Suppression
20. Specific Call Rejection
21. Last Number Dialed
22. IP Telephony Manager (Administrator)
23. IP Telephony Manager (Subscriber)

C.2.2.1.3 Interfaces

The UNIs at the SDP are mandatory unless marked optional.

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP (IETF RFC 3261), H.323, MGCP, or SCCP

C.2.2.1.4 Performance Metrics

The performance levels and AQL of KPIs for IPVS are mandatory unless marked optional.

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Latency	Routine	200 ms	≤ 200 ms	See Note 1
Grade of Service (Packet Loss)	Routine	0.4%	≤ 0.4%	See Note 2
Availability	Routine	99.6%	≥ 99.6%	See Note 3
	Critical	99.9%	≥ 99.9%	
Jitter	Routine	10 ms	≤ 10 ms	See Note 4

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Voice Quality	Routine	Mean Opinion Score (MOS) of 4.0	MOS ≥ 4.0	See Note 5
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 6
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Latency is the average round trip time for a packet to travel from source SDP to destination SDP. This applies to CONUS.
2. Grade of Service (Packet Loss) is defined as the percentages of packets that are sent by the source SDP but never arrive at the destination SDP (the percentage of packets that are dropped).
3. Availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the IPVS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

4. Jitter is the average variation or difference in the delay between received packets of an IP packet data stream from SDP to SDP. Relevant standard: IETF RFC 1889. This applies to CONUS.
5. As defined in ITU-T specification P.800 series.
6. See Section G.8.2 for definition and how to measure.

C.2.2.1.5 Managed LAN Service

The contractor shall provide a Managed LAN Service. The contractor shall provide and manage all LAN networking hardware components (e.g. Layer 2 switching devices, routers, switches, call servers, etc.) to extend the IPVS from the site demarcation point to the terminating user device (e.g., handset), including the management of the router that terminates the IPVS access arrangement. Equipment provided by the contractor shall support Power over Ethernet (PoE) in order to supply necessary power to IP phone sets or other PoE devices. IPVS service is a pre-requisite for Managed LAN Service.

The contractor shall provide, manage, maintain and repair or replace all equipment necessary to provide the Managed LAN Service, except for those portions of the service

for which the government is responsible (e.g., power, facilities, rack space, cabling/wiring).

The contractor shall provide the technical capabilities of the Managed LAN service as specified below:

1. The contractor shall provide all hardware and licensing necessary to extend the IPVS site demarcation point to the terminating device (e.g., the handset), for both hosted and premises-based solutions. In the case of an on-premises solution this includes any hardware or licensing necessary to support on-premises call processing (e.g., call manager, IP PBX, etc.).
2. The contractor's hardware/software solution shall interoperate with the ordering agency's provided VoIP-ready cabling infrastructure, including category 5, 5E, 6, 6A and single mode and multimode fiber at a minimum. The contractor shall identify any cabling limitations with regard to either form of VoIP solution in its proposal.
3. The contractor shall be responsible for the ongoing maintenance and upgrades of the contractor-owned equipment used to provide the Managed LAN Service. If the contractor replaces, makes any changes to the contractor's equipment or device software, or reprograms user devices in order to meet the required service performance level, the government will not incur any additional cost.
4. The contractor shall propose installation time intervals for additional user devices at sites already using a Managed LAN Service.
5. The Managed LAN Service shall not include any wireless devices or components on the LAN (i.e., wired solution only) unless requested and approved by the OCO.
6. The Managed LAN Service shall not support other services (i.e., data, video, etc.) unless requested and approved by the OCO.
7. The contractor shall ensure that only authorized devices (as determined by the ordering agency) are able to operate on the Managed LAN Service.
8. The contractor shall monitor, manage and restore the Managed LAN Service on a 24x7 basis.
9. The contractor shall specify the LAN management activities provided as part of the Managed LAN Service as well as identify those activities which are considered customer responsibilities in the following areas:
    a) Configuration management
    b) Moves, Adds, Changes, Disconnects (MACDs)
    c) Service/Alarm monitoring and fault management
    d) Ticket creation
    e) Proactive notification

f) Trouble isolation and resolution

10. The contractor shall provide proactive notification of major and minor alarms to the Managed LAN Service via e-mail to the Points of Contact (POCs) identified by the ordering agency. Alarm notifications shall be sent to all identified POCs within 15 minutes of alarm detection by the contractor.
11. The contractor shall define the escalation path for trouble tickets for both network and hardware issues. This escalation path shall be identified by level of severity and shall include personnel for each level of escalation as well as guidelines and timing for the next step in escalation.

C.2.2.1.6 Session Initiation Protocol Trunk Service

Session Initiation Protocol (SIP) Trunk Service provides a SIP-based IP Trunk service that interoperates with any Private Branch Exchange (PBX) systems that support SIP-based IP Trunk interfaces.

SIP Trunk Service provides a direct IP connection between a SIP-enabled PBX system on an agency's premises and the contractor's SIP-compliant IPVS network. SIP trunking shall be fully integrated with IPVS to support calling to on-net and off-net locations. The network and its management will be provided by the underlying network service.

C.2.2.1.6.1 Technical Capabilities

The contractor shall provide capabilities that enable SIP users to successfully establish and receive telephone calls between both on-net locations and the PSTN.

C.2.2.1.6.2 Features

The following SIP Trunk Service features are mandatory unless marked optional.

1. Automatic call routing
2. Bandwidth QoS management
3. Trunk bursting
4. Telephone number blocks (DID)

C.2.2.2 Circuit Switched Voice Service

The government has a large community of circuit-switched voice users throughout the US public sector and also conducts a considerable amount of business with US citizens, private sector firms, and foreign entities using circuit-switched voice.

C.2.2.2.1 Service Description

C.2.2.2.1.1 Functional Definition

Circuit Switched Voice Service (CSVS) supports voice calls, whether initiated from on-net or off-net locations, to be connected to all on-net and off-net locations by direct dialing throughout the US. The government's requirement for CSVS is functional.

C.2.2.2.1.2 Standards

The contractor shall comply with voice service industry standards.

C.2.2.2.1.3 Connectivity

CSVS shall connect to and interoperate with:

1. Government-specified terminations (such as single-line telephones, Secure Terminal Equipment, multi-line key telephone systems, conference-room audio equipment, PBX, Centrex, T1 MUX, modem, FAX, and video teleconferencing systems).
2. PSTN, including both wireline and wireless networks, in domestic and non-domestic locations.
3. The voice service networks of all other EIS contractors.
4. Satellite phones and terminals.

C.2.2.2.1.4 Technical Capabilities

The following VS capabilities are mandatory unless marked optional:

1. Numbering plan:
    a) Unique directory number for all on-net government locations, including support for existing government numbers.
    b) PSTN (including both wireline and wireless networks) numbers and any future changes to PSTN numbers.
    c) (Optional) Non-commercial agency-specific private 700 numbers:
        i. Originating and terminating on-net calls. Incoming off-net calls from the PSTN shall be blocked unless an agency-specific request for the service gateway has been received and implemented.
    d) Transparency and interconnectivity between the contractor's network and other networks (see Section C.2.2.2.1.3).

2. Network intercept. Network intercept to a recorded announcement shall be provided as an inherent network capability when a call cannot be completed. At a minimum, such announcements shall be provided for the following conditions:
   a) Number disconnected (a disconnected number shall not be reassigned for at least 90 days if the contractor controls number assignment)
   b) Time-out during dialing
   c) Network congestion
   d) Denial of access to off-net and non-US calls
   e) Denial of access to features
3. (Optional) User-to-user signaling via ISDN D-Channel. The contractor shall support user-to-user signaling in accordance with ITU-TSS Q.931 standards, via the ISDN D-channel during a call.
4. Voice quality at least equal to 64 kbps PCM (standard: ITU G.711).
5. The contractor shall fully comply with emergency service requirements, including 911 and E911 services, and identify the locations of originating stations and route them to the appropriate Public Safety Answering Point (PSAP).

C.2.2.2.2 Features

The following CSVS features are mandatory unless marked optional:

ID Number	Name of Feature	Description
1	Agency-Recorded Message Announcements	1. Authorized government personnel shall be able to record message announcements within the network after authentication of user-ID and password/token. 2. The recording shall be assigned an on-net number and shall be accessible from on-net and off-net stations. 3. The contractor shall provide the capability of a three-minute message announcement length. 4. The length of each message provided by the government will be determined on a case-by-case basis and will continue to three minutes in length (or longer if the contractor capability exists and is provided at no additional cost to the government). 5. A call to the announcement must be answered within five rings and barge-in access to the announcement shall be permitted.

ID Number	Name of Feature	Description
		6. The contractor shall provide a system-wide capability for storing a minimum of 500 recorded messages. This feature shall enable a minimum of 250 callers concurrently to access an announcement.
2 (optional)	Authorization Codes/ Calling Cards	The contractor shall provide authorization codes that support the following functions: 1. Caller identification and class-of-service (CoS) for users to include call screening (see User's Call Screening feature) and service performance levels (see Performance Metrics for routine and critical users). At a minimum, 128 classes of service shall be available to each user, station, or trunk. 2. Same authorization code for originating on-net, off-net, and audio conference calls. 3. Use authorization code if originating station identification cannot be made by other means for billing and CoS purposes. 4. Use authorization code when override capabilities are desired. 5. The CoS derived from an authorization code shall take precedence over that derived from any other means. 6. When an authorization code is used for the service, it shall be verified without involving an operator before a call is connected. 7. The contractor shall support the following capabilities as specified by the government: a. Actual requirements for calling party identification (e.g., ANI suppression). b. CoS assignment. c. Types of calling cards: 1. Post-paid calling cards. (a) Charges accumulate as the card is used, and billing is based upon monthly charges. 2. Pre-paid calling cards. (a) Fixed dollar amount of $50.00

ID Number	Name of Feature	Description
		(b) Rechargeable dollar amount where amount can be renewed or increased when the initial amount balance is low or depleted d. Expiration date for pre-paid calling cards. e. Use for audio conferencing service (ACS) only. f. Agency-specific logo and no printing of GSA logo on the card. g. Suppression of call detail records (CDRs). h. Immediate cancellation of the card if reported stolen or lost by a user without incurring further charges on the card. The format of the authorization code shall be determined by the contractor and shall support/provide the following capabilities: 1. Credit card-sized authorization code card(s), also called Calling Cards, unless otherwise directed by the government. 2. Durable plastic composition and imprinted with authorization code, user's name, and organization. 3. User instructions shall be issued, as directed by the government, at no additional cost. 4. Safeguards as follows: a. Potential fraud and theft regarding issuance, distribution, and activation of authorization codes. b. Delivery of Personal Identification Numbers (PINs) independent from delivery of the calling cards. c. Exclusion of the last 4 digits of authorization codes (i.e., PINs) in billing records. 5. If sufficient space is available, inclusion of the Federal Relay Service's "TDD/800-877-8339" number on the back of the calling card. 6. Contractor-defined dialing sequence that alerts the network when an authorization code is about to be entered so that processing of calls not requiring this feature are not delayed. 7. Temporary override of a CoS restriction assigned to a caller's station. This will allow an individual user to place a call at a higher network CoS for the duration of the call by entering a

ID Number	Name of Feature	Description
		valid authorization code. This capability shall have the following functionalities. a. Absence of excessive delays caused by waiting for all digits to be dialed before recognizing the call as one that involves an override. b. Inclusion of all CDR relevant data charged to the authorization code rather than to the originating station. 8. Allowance of authorized users to gain access, after validation of authorization codes, to on-net voice service and features from off-net locations by dialing certain contractor-provided toll free and message unit-free (to the callers) commercial directory numbers. This capability shall have following functions. a. Numbers may be a local number, a Foreign Exchange number, an NANP number, or some other service type, e.g., toll free service, for which toll free and message unit-free service has been arranged for pre-designated regions. b. Toll free and message unit-free commercial directory numbers shall be printed on the back of the calling card. c. Region boundaries shall be defined by the contractor. d. Users shall be able to select, by service order, the regions of the country from which access is to be allowed and the service type that provides the most economical service for a given application. 9. A multiple call feature that shall allow the user to dial a code (e.g., the “pound” key [#]) after a call in order to make multiple calls without re-dialing the access and card number. 10. Direct operator access to provide assistance with dialing or for providing information. 11. An error correction feature that enables cardholders to correct a dialing mistake by pressing a key, e.g., the “star” key (*) and re-enter the correct number. 12. Speed dialing that allows cardholders to use abbreviated dial codes for frequently dialed numbers.

ID Number	Name of Feature	Description
		13. Availability of all administrative tools or management reports made available by the contractor with equivalent commercial calling card offerings.
3	Caller Identification (ID)	The contractor shall provide the calling number to the terminating stations for each incoming call.
4 4.2. (optional)	Call Screening for users	Call screening consists of a set of features that determine a call's eligibility to be completed as dialed based upon CoS information associated with the user, the station, or the trunk group. The following call screening features shall be supported: 1. Class of Service (CoS) and Restrictions. The contractor shall provide a minimum of 128 classes of service for each user, station, or trunk. CoS shall be determined from the ANI, authorization code, traveling classmark, or trunk group. The CoS derived from an authorization code shall take precedence over that derived from other means. Classes of service shall identify but not be limited to access and feature restrictions as follows: a. Access restrictions shall include but not be limited to access to toll free and 900 calls, access to off-net calling, access to other government networks, access to non-US calling, and access to other than specified NPA/NXXs. b. Feature restrictions shall allow or restrict access to network features by users or groups of users. 2. Code Block. This feature shall screen and prevent ineligible users, stations, and trunks with certain CoS access restrictions from calling specified area codes, exchange codes, and countries. Blocked calls shall be intercepted to appropriate network recorded announcements.
5 (optional)	Customized Network Announcement Intercept Scripts	The contractor shall implement customized network intercept announcement scripts as requested by the government. The contractor shall record the customized network announcements after obtaining government approval of scripts.
6 (optional)	Internal Agency Accounting Code	For calls involving a calling card or originating station with a special CoS, the following capabilities shall be provided: 1. Entry of additional (up to a maximum of eight) digits to identify internal agency accounting codes for the call, i.e.,

ID Number	Name of Feature	Description
		these accounting codes will be transferred to the CDR with no further processing. 2. CDRs shall reflect all relevant data on the call to include internal agency accounting code digits. Calls shall be charged to the authorization code rather than to the originating station.
7	Directory Assistance	A user shall be able to call off-net directory assistance by dialing NPA-555-1212 or any other off-net directory assistance number. NPA also includes service access codes (e.g., 800) for this feature.
8	Suppression of Calling Number Delivery	Based on the CoS of the originating station or calling card, the contractor shall inhibit the delivery of the calling number, i.e., ANI, by setting the Privacy Indicator at the originating end and honoring it at the terminating end. In addition, it shall be possible to block calling number delivery on a call by call basis by dialing a contractor-provided code.
9	Voice Mail Box	The contractor shall offer voice mail capability that includes voice messaging transmission, reception, and storage for 24x7 except for periodic scheduled maintenance. The contractor provided voice mailbox shall meet the following minimum requirements: 1. At least sixty minutes of storage time (or 30 messages) 2. Ability to remotely access voice mail services 3. Secure access to voice mail via a password or PIN 4. Automatic notification when a message is received 5. Minimum message length of two minutes 6. Capability to record custom voice mail greetings This capability can be administered on a station basis according to the ordering agency's needs.
10 (optional)	Basic Subscriber Line: Multi Appearance Directory Number	A Multiple Appearance Directory Number is a telephone number that appears on two or more telephones.
11 (optional)	ISDN PRI: Backup of Shared-D Channel	Backup of a single D channel that is controlling multiple PRIs.

ID Number	Name of Feature	Description
12 (optional)	ISDN BRI: Multi Appearance Directory Number	A Multiple Appearance Directory Number is a telephone number that appears on two or more ISDN telephones.
13 (optional)	MLPP	DOD requires the CSVS to have Multilevel Precedence and Preemption (MLPP) capability as defined in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C and DOD Instruction 8100.3, Department of Defense Voice Networks, to specified users and on trunks connecting to the Defense Switched Network (DSN).

C.2.2.2.3 Interfaces

The UNIs at the SDP are mandatory unless marked optional:

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Analog Line: Two-Wire (Basic Subscriber Line) (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line-Loop Signaling
2	Analog Line: Four-Wire (Basic Subscriber Line) (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line-Loop Signaling
3	Analog Trunk: Two-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk-Loop Signaling (loop and ground start)
4	Analog Trunk: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk–Wink Start Signaling
5	Analog Trunk: Four-Wire	4 kHz Bandwidth	Trunk-E&M Signaling

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
	(Std: Telcordia SR-TSV-002275)		
6	Digital Trunk: T1 (Std: Telcordia SR-TSV-002275 and ANSI T1.102/107/403)	Up to 1.536 Mbps	T1 Robbed-Bit Signaling
7	Digital Trunk: ISDN PRI (23B+D and 24B+0D)T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
8	Digital: T3 Channelized (Std: Telcordia GR-499-CORE)	Up to 43.008 Mbps	SS7, T1 Robbed-Bit Signaling
9 (Non-US)	Digital Trunk: E1 Channelized (Std: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
10 (Optional)	Optical: SONET OC-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	SS7
11 (Optional)	Electrical: SONET STS-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	SS7
12 (Non-US)	Digital: E3 Channelized (Std: ITU-TSS G.702)	Up to 30.72 Mbps	SS7, E1 Signaling
13	Digital Line: ISDN BRI (2B+D) S and T Reference Point	Up to 128 kbps (2x64 kbps)	ITU-TSS Q.931

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
	(Std: ANSI T1.607 and 610)		
14	Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP (IETF RFC 3261), H.323, MGCP, or SCCP

C.2.2.2.4 Performance Metrics

The performance levels and AQL of KPIs for CSVS are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability (POP-to-POP)	Routine	99.95%	≥ 99.95%	See Note 1
Availability (SDP-to-SDP)	Routine	99.5%	≥ 99.5%	
	Critical	99.95%	≥ 99.95%	
Time to Restore	With Dispatch	8 hours	≤ 8 hours	See Note 2
	Without Dispatch	4 hours	≤ 4 hours	
Grade of Service (Call Blockage)	Routine	0.07 (SDP-to-SDP)	≤ 0.07	See Note 3
		0.01 (POP-to-POP)	≤ 0.01	
	Critical	0.01 (SDP-to-SDP & POP-to-POP)	≤ 0.01	

Notes:

1. CSVS availability is calculated as a percentage of the total reporting interval time that the voice service is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

[Note that this KPI is waived for calls made with calling card.]

2. Refer to Section G.8.2 for definition and how to measure.
3. Grade of Service (Call Blockage) is the proportion of calls that cannot be completed during the busy hour because of limits in the call handling capacity of one or more network elements. For example, 0.01 indicates that 1 percent of the calls are not being completed (1 out of 100 calls).

C.2.2.3 Toll Free Service

C.2.2.3.1 Service Description

Agencies can use inbound Toll Free Service (TFS) as a convenient means of accessibility for different callers including citizens, non-citizens, and agency personnel. TFS includes a set of advanced service features and related voice applications to meet agency needs for delivering services to their callers.

C.2.2.3.1.1 Functional Definition

Toll Free Service provides basic inbound toll free calling and offers advanced feature and call routing capabilities. TFS includes intelligent call routing and network-based Interactive Voice Response (IVR) capabilities to enable agencies to effectively manage inbound calls.

C.2.2.3.1.2 Standards

Toll Free Service shall comply with the following standards:

1. ITU-T standard E.164 as interpreted by the Industry Number Committee of the Alliance for Telecommunications Industry Solutions (ATIS). The contractor shall support the following numbering schemes:
   a) For domestic (CONUS and OCONUS) service, numbering shall be consistent with 800, 888, 877, 866, and other toll-free non-geographic codes available from the SMS/800 database managed by Telcordia.
   b) For non-domestic service, numbering shall be consistent with requirements or practices in the country in which the call originates.
2. ITU-T P.800 series of standards for telephone transmission quality.
3. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards.

C.2.2.3.1.3 Connectivity

Toll Free Service shall connect to and interoperate with the PSTN including both wireline and wireless. TFS uses underlying Voice Service for connectivity as delineated in Section C.2.2.2.1. TFS shall be provided for both dedicated and switched terminating access arrangements.

C.2.2.3.1.4 Technical Capabilities

The following TFS capabilities are mandatory unless marked optional.

1. The contractor shall act as the responsible organization or “Resp Org” for assignment and maintenance of toll-free numbers if requested by the ordering agency.
2. The contractor shall support toll-free number portability.
3. The contractor shall accommodate any presently assigned agency toll-free numbers.
4. When requested by an ordering agency, the contractor shall offer Universal International Toll-Free Number service (also known as Universal International Free Phone Number - UIFN). This shall enable the agency to request a single, unique toll-free number that is the same throughout the world (where available commercially from participating countries).
5. The contractor shall provide the capability for a single toll-free number to terminate at multiple locations (SDPs) and multiple toll-free numbers to terminate at a single location (SDP).
6. As a default measure, the contractor shall provide a busy signal or recorded announcement for all calls that encounter network congestion and/or terminating egress congestion, as determined by the ordering agency.
7. The contractor shall provide a network intercept to record announcements as an inherent network capability when a call cannot be completed. At a minimum, such generic announcements shall be provided for the following conditions:
   a) Time out during dialing
   b) Denial of access to features and other related conditions
   c) Denial of access to non-domestic or restricted calls
8. The contractor shall provide the capability for customized network intercept recorded announcements. The contractor shall provide options for the custom announcement to be a) recorded by the contractor or b) recorded remotely by the ordering agency.

9. The contractor shall, at a minimum, provide the capability to have all announcements recorded in English and Spanish languages. Other languages shall be optional.
10. The contractor shall provide a referral message to callers of a disconnected toll-free number. Upon a submission of a TFS disconnect order; the agency shall have the option for a referral telephone number to be provided in an announcement message to callers of the disconnected toll-free number.
11. The contractor shall provide Dialed Number Identification Service (DNIS). DNIS will enable multiple toll-free numbers to be routed and uniquely identified on a shared trunk group. The contractor shall transmit DNIS digits, upon agency request, prior to the delivery of a TFS call to uniquely identify the dialed toll-free number. The DNIS digit length shall range from 3 to a maximum of 10 digits.
12. The contractor shall identify and provide the calling parties Automatic Number Identification (ANI) to assist agencies with identifying malicious or emergency calls.

C.2.2.3.2 Features

The following Toll Free Service features are mandatory unless marked optional.

These features shall be capable of being used independently of each other or in any combination except where noted in the contract. The combination of features associated with routing functions unique with each toll-free number shall constitute a “Call Routing Plan.” Call Routing Plans shall be subject to control by the ordering agency via the Routing Control feature described in this section.

ID Number	Name of Feature	Description
1	Agency-based routing database (also known as Host Connect)	The contractor shall provide the ability to route TFS calls or provide information based upon a query(s) of information provided by a database located at the ordering agency premises. The query(s) could be to single, redundant, or multiple databases, depending upon agency specifications and the complexity of the application. The contractor shall implement and provide the appropriate interface and connectivity for the contractor’s IVR application to successfully query and access an ordering agency’s database(s). The IVR caller shall have the capability to retrieve, review, and modify information located on the agency database based upon ordering agency needs. The agency database(s) can be a (1) mainframe or (2) server-based relational database.

ID Number	Name of Feature	Description
		If the database does not respond to the network query within 250 milliseconds, an agency-defined default routing plan shall be used.
2	Alternate Routing (also known as "Cascade" routing)	The contractor shall allow TFS calls to be re-routed on a pre-determined plan based upon availability of trunks (busy) at the terminating location, a maximum number of calls allowed in progress, or a pre-defined ring-no-answer condition. If none of the alternate terminations are able to receive the call, then the call shall be terminated to (1) a predefined announcement, or (2) a busy signal, at the ordering agency's option.
3	ANI	Automatic Number Identification (ANI). The contractor shall allow transmission of the TFS caller's real time ANI information (full 10 digit number or non-domestic equivalent) to the ordering agency.
4	ANI Based Routing	The contractor shall enable TFS calls to be routed based upon the originating ANI of the caller. Default routing defined by the ordering agency shall be used if ANI is not available.
5	Announced Connect	The contractor shall provide a customized message to the called party, before the TFS caller is connected, and provide the called party with information about the caller (e.g. ANI, account number etc.). This feature is commonly referred to as a "whisper."
6	Announcements	The contractor shall provide TFS network-based announcements with both generic and customized recordings. For customized recordings, the agency shall have the option to record the custom announcement script or have the contractor record the script. At a minimum, the announcements should be available in (1) English, (2) Spanish, and (3) (optional) other languages. At an agency's request, the contractor shall provide the option for a forced disconnect after the announcement recording is played.
7	Menu Routing	The contractor shall allow TFS callers to be provided with informational messages and be routed according to information entered via DTMF signal or via speech. The contractor's call prompter shall provide, at a minimum, the following capabilities: 1. Select pre-recorded announcement messages with the capability for announcements. Such announcements shall always be played from the beginning for each caller and provide the capability to be recorded in English and other languages after obtaining ordering agency script approval.

ID Number	Name of Feature	Description
		2. The contractor shall provide the ability to transfer out ("menu routing") during an announcement to an agency-specified predefined termination with an option to return back an announcement/menu without needing to redial. 3. The contractor shall support multi-tiered prompting (menus) such that another series of options can be provided to the caller after making the initial menu selection, and provide routing to an agency designed default location if no caller input is entered. 4. The contractor shall provide the ability for the caller to leave information via DTMF signal or speech (e.g., names, addresses, account information, phone numbers) for transcription or reporting purposes. For speech transcription, the contractor shall provide a) transmission of the recorded voice files and DTMF data for each transaction to the agency and b) a report of caller responses that transcribes the caller provided information for the ordering agency based upon an ordering agency's needs and transmits it to the agency. The contractor shall provide transcription reports from English and Spanish speaking callers. 5. The contractor shall provide a capability that allows callers to hear and verify their names and addresses in an agency-provided name and address database after the caller has entered his or her telephone number via DTMF, or based on the caller's ANI. 6. The contractor shall provide a means for the ordering agency to retrieve caller-entered DTMF or speech messages. 7. Upon agency request, the contractor shall offer the option for a forced disconnect after an announcement recording is played.
8	Call Redirection	The contractor shall enable TFS calls to be transferred by the contractor's network, no matter which platform the call is being re-directed from, from the called party/agent to another toll-free number or any PSTN number by using, at the agency's discretion, any one of the three following modes of network level call transfer: 1. Blind transfer (unsupervised) 2. Verification by the agent and then transfer (supervised) 3. Three-way conference and then transfer The contractor shall ensure that there is no double billing for toll free calls that have been transferred using call redirection. This

ID Number	Name of Feature	Description
		includes calls redirected within the contractor's network from one operating platform to another operating platform. In addition, the contractor shall offer the ability to put the caller on hold and provide abbreviated dialing codes. The contractor shall state the amount of abbreviated-dial codes available for use with this feature. The contractor shall provide two options for music on hold during the call redirection – either contractor provided or from an agency-provided source.
9	Computer Telephony Integration (CTI)	The contractor shall provide CTI messaging capability that enables transfer of caller information and agency-specified data between the TFS contractor and agency-specified systems simultaneously with the associated inbound toll-free call. This feature can be used to support a diverse set of applications such as screen pop/splash, intelligent call routing, enhanced reporting, third party call control and multi-channel call blending solutions.
10	Custom Call Records	This feature shall be used in conjunction with the TFS Interactive Voice Response and Call Prompter features. The contractor shall provide individual call detail data records which include, at a minimum, the following data: 1. Date and time of TFS call 2. Call duration 3. Specific details regarding the call attempt (e.g., menu options selected in an IVR or Call Prompter application) 4. Call entered digits 5. Call disposition (busy, complete, no answer, blocked) 6. Caller information (ANI - if available or DNIS) 7. Toll-free number dialed 8. Flexible custom fields according to agency needs The contractor shall provide a detailed description of each call detail record field including definitions of the data elements prior to activation of the feature. The format of the call record data shall be such that it can be easily imported into agency databases or applications. The call records and a summary report should be available electronically on a daily, weekly or monthly basis as requested by the ordering agency.
11	Day of Week Routing	This contractor shall enable TFS calls to be routed to different terminations or applications based upon the day of week.

ID Number	Name of Feature	Description
12	Day of Year Routing (Holiday Routing)	The contractor shall enable TFS calls to be routed to different terminations or applications based upon the day of the year. A minimum of ten dates should be eligible during a twelve month period for day of year routing.
13	In Route Announcements	This feature shall allow TFS callers to hear an announcement during call setup without affecting the final termination/route of the call. At a minimum, announcements shall be available in either (1) English or (2) Spanish and (3) (optional) other languages.
14	Interactive Voice Response (IVR)	The contractor shall provide an automated application that provides TFS callers with information based upon input from either (a) DTMF key entries or (b).natural speech recognition. The contractor shall provide the minimum required capabilities listed below: 1. Select pre-recorded announcement messages with the capability for announcements and offer the ability for a caller to opt out during an announcement to a predefined termination and an option to return back an announcement without needing to redial. Such announcements shall always be played from the beginning for each caller and provide the capability to be recorded in English and other languages. 2. Leave caller information via DTMF signal or speech (e.g., name, address, account information, etc.). For transcription of caller information, the contractor shall provide a) transmission of the recorded voice files and DTMF data to the agency and b) a report of caller responses that transcribes the caller provided information for the ordering agency based upon the ordering agency's needs and transmits it to the agency. The contractor shall provide transcription reports from English and Spanish speaking callers. 3. The contractor shall provide a means for the ordering agency to retrieve caller-entered DTMF or speech messages. 4. The contractor shall query a database that delivers agency-provided information to the caller. The database may be located at the ordering agency or, at the ordering agency's discretion, located at a contractor location and updated by the ordering agency. Provide a default routing or message (agency option) if the database is unavailable. 5. The contractor shall provide a capability to allow callers to hear and verify their names and addresses in an agency-

ID Number	Name of Feature	Description
		provided name, address, and zip code database after the caller has entered his or her telephone number via DTMF, or based on the caller's ANI (Text to Speech). 6. The contractor shall support speech recognition as a valid caller input. The contractor shall support at a minimum, all spoken numeric digits as well as "yes" and "no." English and Spanish language callers shall be supported. The contractor shall be able to accept and process, at a minimum, 95% of the above speech responses. Speech responses which are not accepted shall be routed to default location designated by the ordering agency. 7. The contractor shall provide the capability to perform surveys (via DTMF or speech) to IVR callers. The surveys can be provided to all or a random percentage of callers according to agency needs. Survey results shall be provided electronically to the ordering agency. 8. (Optional) The contractor shall provide a facsimile or technical equivalent "fax back" capability (Fax or equivalent) that shall permit callers to retrieve agency-specific documents or forms. The contractor shall fax back the request documents within one hour of the initial call and retry a minimum of 13 attempts over a six hour interval in order to complete the request. Fax or technical equivalent transmittal shall include an option for a cover sheet (standard or customized). 9. At the agency's option, the caller's IVR selection(s) information shall be transferred to the agency. 10. The contractor's IVR capacity must be configured such that the application answers a call within 3 ring cycles for 99 % of the offered call volume (measured on an hourly basis) during the busy hour. 11. The contractor shall provide features equivalent to the above shall be available to individuals who are hearing impaired or have speech disabilities via electronic means in Baudot and ASCII/TTY code formats. These electronic form lines need not be voice feature enabled. 12 The contractor shall provide summary reporting that at a minimum provides information on the caller, average call duration, caller opt out (transfer), and disposition of the calls within the IVR application on a daily, weekly, and monthly basis.

ID Number	Name of Feature	Description
15	Make Busy Arrangement	The contractor shall permit the agency to deactivate one or more TFS dedicated access trunks within a trunk group, Upon deactivation, the trunk(s) shall appear in a busy state. The capability to activate and deactivate the status of the trunks shall be controlled either via software available to the ordering agency or at the agency's option by notifying the contractor. At a minimum, the request shall be executed by the contractor within one hour of request.
16	Network Call Distributor	The contractor shall provide advanced, intelligent call routing capabilities based upon real time status of each contact center's operating conditions, agent skills, and/or agency-specified business rules. The contractor shall poll all of the ordering agency's PBX/ACD's regular intervals for real-time ACD operating status information to update a call routing processor which shall use call routing logic/algorithms that have been predefined by the agency, to determine the best location or resource to deliver the inbound call. The call routing processor containing the call routing logic/algorithms shall be able to use, in the ordering agency's defined combinations, all real-time operating status information collected from the agency's PBX/ACD's. The ACD-provided information shall be polled and shall include at a minimum: 1. Number of incoming trunks 2. Number of incoming trunks available to receive a call 3. Number of calls in queue or queue size 4. Average delay in queue 5. Number of answering agents logged on 6. Number of answering agents unavailable to answer a call 7. Number of answering agents available to answer a call 8. Number of answering agents available to answer a call by skill 9. Longest available answering agent 10. Average speed of answer 11. Average call handling time (includes agent talk time, after-call wrap-up time and call hold time) 12. Number of calls abandoned 13. Average time to abandonment

ID Number	Name of Feature	Description
		The type of network information that shall also be available to the call routing processor for utilization by the call routing logic/algorithms shall include: 1. The dialed toll-free number 2. The caller's originating 10 digit number 3. The caller's entered digits. Call routing logic/algorithms that shall be accommodated shall include at a minimum: 1. Routing to the best available answering agent by skill group 2. Routing based upon expected wait times 3. Routing based upon least cost. The contractor shall document the maximum hourly call processing rate and grade of service available without any degradation in performance (e.g. can process 100,000 calls per hour). The contractor shall permit the call routing processor up to 250 milliseconds from receipt of a call query to respond to the destination (or next node). In the event that 250 milliseconds are exceeded, the contractor shall route the call using a default routing plan previously defined by the ordering agency. The contractor shall provide, via a graphical user interface, all software and hardware necessary for agency access to the call routing processor to permit agency definition of the call routing logic/algorithms. The ordering agency will be responsible for providing telecommunications connections to the contractor's system. The Network Call Distributor feature shall be offered as a managed service with the following options: 1. Contractor-provided and contractor-based: The contractor shall provide all necessary components required for the provision of this feature and they shall be housed within the contractor's network. (Default). 2. Contractor-provided and agency-based: The contractor shall provide all necessary components required for the provision of this feature and they shall be housed at the ordering agency's designated location (Where applicable). The contractor shall provide any additional reporting or monitoring options that are available from the contractor's equivalent commercial service offering at no additional charge.

ID Number	Name of Feature	Description
17 (Optional)	Network Queuing	The contractor shall enable TFS callers to remain, in a network queue, if resources are unavailable at the ordering agency. This is a feature that shall allow a caller to be held in queue in the contractor's network until an ordering agency's terminating SDP(s) become(s) available to receive the call. Upon entering the queue, the caller shall hear an initial announcement and shall then hear a reassurance announcement at a predetermined interval thereafter. The ordering agency shall be able to define the time for calls that can be held in queue before being sent to a terminating announcement. The contractor shall be responsible for recording announcements after ordering agency script approval.
18	NPA/NXX Routing	The contractor shall enable TFS calls to be routed to different terminations based upon the calling party's originating NPA or NPA/NXX or country code. Where NPA/NXX is not available, calls shall be routed to an agency-defined default location.
19	Percentage Call Allocation	The contractor shall enable TFS calls to be allocated on a percentage basis and terminate at multiple locations. The agency-specified percentage distribution can range from 0% to 100% in a minimum of 1% increments.
20	Real Time Reporting	The contractor shall provide agencies with the ability to monitor and report on summary and detail data relating to the status of TFS calls on a near real-time basis (e.g., minimum required refresh rate of 30 seconds and at other contractor proposed intervals). The TFS reports and monitoring data shall be available electronically within 5 minutes of the request. The contractor shall provide all components necessary to present this information in a graphical and tabular format to the ordering agency and allow it to be exported to external applications (e.g., spreadsheet or database). The user will be responsible for providing connections to the contractor's real time monitoring system. A secure web based-interface is preferred. At a minimum, the contractor shall provide the following: 1. The number of TFS calls from each area code who have dialed a given toll free number and average call duration. 2. The total number of calls directed to an ordering agency's terminating SDP. 3. The total number of calls directed to an ordering agency's terminating SDP(s) that could and could not be completed.

ID Number	Name of Feature	Description
		4. The percentage of trunks busy at a user's terminating SDP. 5. Any standard real time reports or data available to commercial users. The contractor shall make available any reports available from its corresponding commercial service offering.
21	Routing Control	The contractor shall allow ordering agencies to perform real time and scheduled TFS call routing changes from their location or via the contractor's customer service center. This feature shall permit authorized users to review, create, validate, change, or execute call routing plans (or sets) from the ordering agency's premises or via request to the contractor's customer service center. Activation of a routing plan shall be executed in a period not to exceed 5 minutes of the request. 1. The contractor shall provide adequate security procedures that will prevent unauthorized access to this feature. 2. The contractor shall provide audit trail information to track the identity, time, and plan changes executed by a user. 3. The contractor shall provide any components necessary to enable the user to use this feature. 4. Users may provide their own terminal equipment when it meets contractor-provided specifications.
22	Service Assurance Routing	The contractor shall route TFS calls to an announcement or a predefined alternate termination within five minutes of the agency request if an emergency situation or service disruption occurs. The contractor shall complete routing requests to other types of terminations within thirty minutes of the request.
23	Speech Recognition	The contractor shall provide network based natural speech recognition applications with the ability to recognize spoken vocabulary, digits, zip codes, credit card numbers, account numbers, alpha numeric numbers, etc. At a minimum, the contractor shall offer capabilities in (a) English, (b) Spanish and (c) (optional) other languages.
24	Tailored Call Coverage	The contractor shall enable restriction of TFS calls originating from specific areas (country, state), telephone numbers (NPA, NPA/NXX, or ANI), or call type (Payphones). The originating caller should hear a standard announcement informing them of the restriction.

ID Number	Name of Feature	Description
25	Time of Day Routing	The contractor shall enable routing of TFS calls to different terminations or applications based upon the time-of-day. At a minimum, at least 48 time-of-day intervals shall be offered.
26	Language Interpretation Service	The contractor shall provide language translation services to support near-real time communications between callers speaking different languages.
27	Virtual Queue	The contractor shall provide a capability whereby callers can choose to remain waiting on-line for an attendant or receive a call back in turn.
28	Vanity Toll Free Number	The contractor shall provide agency-requested “vanity” toll-free numbers (e.g., 1-800-CALL-GSA), if available.

C.2.2.3.2.1 TFS Feature Reports

At the request of the ordering agency the contractor shall provide TFS reports that provide the ordering agency with information about the status of calls placed to each toll free number and/or termination. The reports shall capture this information on an (1) hourly, (2) daily, (3) weekly, (4) monthly, and (5) quarterly basis. Reports shall contain information summarized in 30- and 60-minute increments. Multiple report formats that further summarize the information by time zone or ordering agency region shall be made available where applicable. The reports shall be archived and available for a minimum of 90 days.

Reports shall be made available by electronic means such as a web site, or via e-mail or other contractor-proposed applications and have the capability to export data, in a standard file format, to agency applications (e.g., spreadsheets, databases) for analysis. The reports shall be made available electronically within 30 minutes of the submitted request. The contractor shall also provide agencies with documentation containing a description of the report, definition of the report fields, and instructions on how the agency can effectively use the report(s) to manage TFS.

All time indicators within the report shall default to Eastern Time with presentation of hours using either a 24-hour clock or a 12-hour clock with an AM/PM indicator. There shall also be an option to provide the reports indicating the time zone of the TFS terminating location.

Each report shall contain standard information including:

1. Title of Report
2. Date of Report
3. Period covered by the Report
4. Name of ordering agency
5. Toll free number(s) included in the Report

Listed below are the minimum reporting requirements. They are mandatory unless marked optional. The contractor shall also provide any historical or real-time reports that are available with its TFS reporting packages.

ID Number	Name of Feature	Description
1	Call Status Report – Toll Free Service	For any given toll free number, the contractor shall, at a minimum, provide the following information within the reports: 1. The number of call attempts from each area code and/or State that dialed the toll free number. A minimum of three views shall be available: a. calls originated by area code b. calls originated by State c. sorted by State and area code 2. The number of calls and the percentage of all calls that encounter a busy signal or that are blocked: a. Within the contractor's TFS network b. At the user's (agency's) terminating access location 3. The number of calls offered to the user TFS trunk group 4. The number of calls received at each user's terminating access 5. The number of received calls at each user's terminating access that resulted in successful answerback supervision 6.The average duration of calls answered at each user's terminating access 7. The average duration of all calls answered for a given toll free number at all terminations serving the toll free number.
2	Call Status Report – Alternate Routing	For any given toll free number utilizing Alternate Routing, the contractor shall, at a minimum, provide the following information within the reports:

ID Number	Name of Feature	Description
		1. The total number of calls offered to the initial termination 2. The number of calls that were re-routed to alternate SDP(s) or toll free service trunk group(s).
3	Call Status Report – Announcement	For any given toll free number utilizing Terminating Announcement or In-Route Announcements, the contractor shall, at a minimum, provide the following information within the reports: 1. The number of calls offered to the announcement 2. The number of calls blocked at the announcement 3. The number of calls completed in the announcement 4. The average duration of calls to each announcement 5. The number of abandoned calls for In-Route announcements.
4	Call Status Report – Call Prompter	For any given toll free number utilizing Call Prompter Access, the contractor shall, at a minimum, provide the following information within the reports: 1. The number of calls offered to the call prompter 2. The number of calls to the call prompter that were abandoned without making a selection 3. The average duration of all calls while in the call prompter 4. The number and percentage of calls selecting each option within the call prompter application.
5	Call Status Report - IVR	For any given toll free number utilizing IVR, the contractor shall, at a minimum, provide the following information within the reports by application: 1. The total number of calls offered to the IVR and average call duration 2. The number of calls completed (i.e., successfully accessed) to the IVR 3. The number and percentage of calls completed to the IVR but abandoned within the application 4. The number and percentage of calls selecting each option 5. The average duration of calls selecting each option 6. For faxback applications, the fax delivery status and usage

ID Number	Name of Feature	Description
		7. For survey applications, summary and detail information on call survey responses 8. For transcription applications, summary and detail information regarding transcription usage.
6	Caller Information Report	The contractor shall provide a report that identifies the ANI information of all callers to a specified toll free number. Note: agencies recognize that ANI, although available in most cases, is not always provided. In those instances where ANI is not available, the NPA or NPA-NXX (as available) of the caller shall be provided. Zeroes shall be substituted in place of any missing digits. For any given toll free number, the contractor shall, at a minimum, provide the following information regarding each call: 1. Date of call 2. Time of call (expressed using either a 24 hour clock or a 12 hour clock with an AM/PM indicator, Eastern Standard Time) 3. ANI of caller (if available) 4. Dialed 10 digit number 5. Duration of call 6. Disposition of call (i.e., using an alpha or numeric code) to include, at a minimum, the following information: a. Call blocked within contractor's network b. Call blocked at user's terminating access c. Call completed to user's terminating access d. Other (not included in categories a – c above)
7	Caller Profile Report	The contractor shall provide the following caller information: 1. Lost Callers. The number of TFS callers who never called back after an incomplete attempt during the reporting period. 2. Average Number of Attempts Per Caller. The grand total number of call attempts divided by the number of first call attempts during the reporting period. 3. Average Number of Contacts Per Caller. The number of attempts generated from each telephone number on average during this reporting period. This is calculated by dividing the total number of first call attempts by the total number of unique telephone numbers from which the calls were made.

ID Number	Name of Feature	Description
		4. 50 Percent of Successful Attempts. Represents the number of attempts to access the network for 50 % of the callers who completed during the requested measurement interval. 5. 75 Percent of Successful Attempts. Represents the number of attempts it took to access the network for 75 % of the callers who completed during the requested interval.
8 (optional)	Call Redirection Report	The contractor shall provide a summary report on the call redirection activity by toll free number and abbreviated dial code (if applicable). At a minimum, the report should identify the following: 1. Number of transfer attempts 2. Number of completed transfers 3. Number of incomplete transfers 4. Number of blocked transfers 5. Type of call redirection (blind, supervised, or 3 way) 6. Terminating number for redirection

C.2.2.3.3 Interfaces

The UNIs at the SDP, as defined below, are mandatory unless marked optional.

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1 (Optional)	Analog Line: Two-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line-Loop Signaling
2 (Optional)	Analog Line: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line-Loop Signaling
3	Analog Trunk: Two-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk-Loop Signaling (loop and ground start)

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
4	Analog Trunk: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk-E&M Signaling, Wink Start Signaling
5	Digital Trunk: T1 (Std: Telcordia SR-TSV-002275 and ANSI T1.102/107/403)	Up to 1.536 Mbps	T1 Robbed-Bit Signaling
6	Digital Trunk: ISDN PRI T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
7	Digital: T3 Channelized (Std: Telcordia GR-499-CORE)	Up to 43.008 Mbps	SS7, T1 Robbed-Bit Signaling
8 (Non-Domestic)	Digital Trunk: E1 Channelized (Std: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
9 (Optional)	Optical: SONET OC-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	SS7
10 (Non-Domestic)	Digital: E3 Channelized (Std: ITU-TSS G.702)	Up to 30.72 Mbps	SS7, E1 Signaling
11	Digital Line: ISDN BRI S and T Reference Point (Std: ANSI T1.607 and 610)	Up to 128 Kbps (2x64 Kbps)	ITU-TSS Q.931

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
12	Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP (IETF RFC 3261), H.323, MGCP, or SCCP

C.2.2.3.4 Performance Metrics

The performance levels and AQL of KPIs for Toll Free Service below are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Av(POP-to-POP)	Routine	99.95%	≥ 99.95%	See Note 1
Av(POP-to-terminating SDP)	Routine	99.5%	≥ 99.5%	
	Critical	99.95%	≥ 99.95%	
Grade of Service (Call Blockage)	Routine	0.07	≤ 0.07	See Note 2
	Critical	0.01	≤ 0.01	
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 3
	With Dispatch	8 hours	≤ 8 hours	

The performance metrics for TFS are based upon underlying service derived from Section C.2.2.2 Circuit Switched Voice Service.

Notes:

1. Av (POP-to-POP) and Av (POP-to-terminating SDP) are measured and calculated as a percentage of the total reporting interval time that TFS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Grade of Service (Call Blockage) is the proportion of calls that cannot be completed during the busy hour because of limits in the call handling capacity within the contractor's TFS. For example, 0.01 indicates that 1 percent of the calls are not being completed successfully (1 out of 100 calls).
3. See Section G.8.2 for the definitions and measurement guidelines.

C.2.2.4 Circuit Switched Data Service

C.2.2.4.1 Service Description

Requirements for digital connectivity on a dial-up basis will continue. The government continues to support a community of CSDS users, particularly in the area of on-demand video conferencing applications.

C.2.2.4.1.1 Functional Definition

CSDS provides a synchronous, full duplex, totally digital, circuit-switched service at multiple data rates, including integral multiples of DS0 data rates (i.e., NxDS0, where N = 1 to 24) to on-net and off-net locations.

C.2.2.4.1.2 Standards

CSDS shall comply with the following standards:

1. ANSI X3.189
2. ITU E.721
3. Applicable Telcordia and ANSI standards for digital transmission, including SONET
4. ITU-TSS and EIA standards for DTE interfaces

C.2.2.4.1.3 Connectivity

CSDS shall connect to and interoperate with:

1. Agency-specified terminations such as Digital PBX, Intelligent MUX, Group 4 FAX, Video CODEC, and Workstation/PC
2. PSTN (where available)
3. All other EIS CSDS contractors' networks

C.2.2.4.1.4 Technical Capabilities

The following CSDS capabilities are mandatory

1. Uniform numbering plan:
   a) Unique directory number for all on-net government locations
   b) Same uniform numbering plan as proposed for VS and which shall be integrated with the VS plan (See Section C.2.2.2.1.4)
2. Authorization Codes for CSDS. Authorization codes for CSDS shall be the same as those specified for VS (see Section C.2.2.2.2 #1 and #2, Features Authorization Codes).
3. For calls terminating to off-net locations, the bandwidth requested by the originating on-net location shall be limited to the bandwidth limitations in the PSTN between the contractor's network and the called location.
4. Calling capability that does not require scheduling.
5. Provision of network-derived clocking to the DTE or PBX/Multiplexer (MUX) at the SDP.
6. Following call establishment, all bit sequences transmitted by the DTE shall be transported as data/bit transparent and shall maintain data/bit sequence integrity.
7. Categories of dialable information-payload bandwidth are as follows:
   a) DS0 Category. The dialable bandwidth shall be DS0 (i.e., 56 kbps and 64 Kbps) data rate
   b) DS1 Category. The dialable bandwidth shall be DS1 (i.e., 1.536 Mbps) data rate
   c) Multirate DS0 Category. The dialable bandwidth shall be NxDS0, where N= 1 to 24
8. For the Multirate DS0 category, the contractor shall provide the following:
   a) Appropriate dialing sequence for initiating calls with different bandwidths
   b) Transport of all bit sequences transmitted by the DTE as data/bit transparent after establishment of the dialing sequence

The following categories of dialable information-payload bandwidth are optional:

1. Multirate DS1 Category. The dialable bandwidth range shall be available from DS1 to N times DS1 data rates, where N varies from 2 to 27.
2. DS3 Category. The dialable bandwidth shall be DS3 (i.e., 43.008 Mbps) data rate.

3. SONET Level-I (i.e., OC-1) Category. The dialable information-payload bandwidth shall be SONET OC-1 (i.e., 49.536 Mbps) data rate.
4. SONET Level-II (i.e., Multirate OC-1) Category. The dialable information-payload bandwidth range shall be available from SONET OC-1 to N times OC-1 data rates (concatenated), where N varies from two to three.
5. SONET Level-III (i.e., Multirate OC-3) Category. The dialable information-payload bandwidth range shall be available from SONET OC-3c to N times OC-3c data rates (concatenated), where N varies from two to four. SONET OC-3c shall support information-payload data-rate of 148.608 Mbps.

C.2.2.4.2 Features

The following CSDS features are optional:

ID Number	Name of Feature	Description
1	Dial-In	The contractor shall support toll-free numbers, in addition to 10-digit PSN numbers, for dial-in access from off-net locations (i.e., PSN) via ISDN access arrangement. Access to CSDS shall only be provided after verification of the authorization code entered by the user.
2	User-to-User Signaling Via ISDN D-Channel	User-to-user signaling via ISDN D-channel during a call shall be supported in accordance with ANSI T1 and ITU-TSS standards for ISDN and SS7.

C.2.2.4.3 Interfaces

The following UNIs at the SDP are mandatory unless marked optional:

UNI Type	Interface Type and Standards	Payload Data Rate	Signaling Type
1	ITU-TSS V.35	Up to 1.536 Mbps	RS366A (dialing)
2	EIA RS-449	Up to 1.536 Mbps	RS366A (dialing)
3	EIA RS-530	Up to 1.536 Mbps	RS366A (dialing)
4	ISDN PRI (Multirate) (T Reference Point) (Standard: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931

UNI Type	Interface Type and Standards	Payload Data Rate	Signaling Type
5	T1 (with ESF) (Std: SR-TSV-002275, and ANSI T1.102/107/403)	Up to 1.536 Mbps	SS7
6 (Optional)	T3 (Standard: Telcordia Pub GR-499-CORE)	Up to 43.008 Mbps	SS7
7 (Optional)	E1 (Standard: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
8 (Optional)	E3 (Standard: ITU-TSS G.702)	Up to 30.72 Mbps	SS7, E1 Signaling
9 (Optional)	Optical: SONET OC-1 (Standard: ANSI T1.105 and 106)	Up to 49.536 Mbps	SS7
10 (Optional)	Electrical: SONET STS-1 (Standard: ANSI T1.105 and 106)	Up to 49.536 Mbps	SS7
11 (Optional)	SONET OC-3 (Standard: ANSI T1.105 and 106)	Up to 148.608 Mbps	SS7
12 (Optional)	SONET OC-12 (Standard: ANSI T1.105 and 106)	Up to 594.432 Mbps	SS7
13 (Optional)	ISDN BRI (Multirate) (S and T Reference Point) (Standard: ANSI T1.607 and 610)	Up to 128 Kbps	ITU-TSS Q.931

C.2.2.4.4 Performance Metrics

The performance levels and AQL of KPIs for CSDS are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability (POP-to-POP)	Routine	99.95%	≥ 99.95%	See Note 1
Availability (SDP-to-SDP)	Routine	99.5%	≥ 99.5%	
	Critical	99.95%	≥ 99.95%	
Time to Restore	With Dispatch	8 hours	≤ 8 hours	See Note 2
	Without Dispatch	4 hours	≤ 4 hours	
Grade of Service (Call Blockage)	Routine	0.07 (SDP-to-SDP)	≤0.07	See Note 3
		0.01 (POP-to-POP)	≤ 0.01	
	Critical	0.01 (SDP-to-SDP & POP-to-POP)	≤ 0.01	

Notes:

1. CSDS availability is calculated as a percentage of the total reporting interval time that CSDS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Refer to Section G.8.2 for definition and how to measure.
3. Grade of Service (Call Blockage) is the proportion of calls that cannot be completed during the busy hour because of limits in the call handling capacity of one or more network elements (e.g., “All trunks busy” condition). For example, 0.01 indicates that 1 percent of the calls are not being completed (1 out of 100 calls).

C.2.3 Contact Center Service

C.2.3.1 Service Description

Contact Center Service (CCS) provides services and personnel to enable agencies to deliver customer service to their clientele across multiple contact channels (voice, fax, email, Internet web site, SMS, chat, etc.) by providing a single network call queue or multiple call queues (where applicable). A network call queue manages multimedia customer interactions such as voice, email, web submissions, and fax. The call queue(s) provides the consistent, real-time management and distribution of multi-media calls to an agency contact center. CCS may be used in conjunction with toll-free and other network services to facilitate agency communications with the general public, businesses, and other agencies. CCS also offers a call answering service with the call queue. The CCS call answering service enables the agency to use contractor-provided resources to respond to caller inquiries. The contractor-provided call answering resources can be located at either 1) an agency location(s) or 2) a contractor location(s).

C.2.3.1.1 Functional Definition

CCS can enable ordering agencies to deliver customer service to their designated customer base across multi-media contact channels (voice, fax, email, web site, etc.) and provide additional enabling services for end-to-end customer service. The basic service provides intelligent call routing capabilities with a network call queue. CCS will apply to single site, multiple site, and enterprise-wide agency contact centers.

C.2.3.1.2 Standards

The following CCS standards are mandatory unless marked optional:

1. (Optional) Computer Supported Telephony Applications (CSTA)
2. IETF RFC's for IPv4 and IPv6
3. ITU-T H.248.1 / Megaco (IETF RFC 3525)
4. ITU-T H.323
5. ITU-T T.30, T.37, T.38, and T.120
6. (Optional) Skinny Client Control Protocol (SCCP)
7. IETF RFC 3261 for Session Initiation Protocol (SIP)
8. Voice eXtensible Markup Language (VxML)
9. All appropriate standards for any underlying access and transport services.

The contractor shall comply with all new versions, amendments, and modifications made to the above listed documents and standards.

C.2.3.1.3 Connectivity

CCS shall connect and interoperate with PSTN.

C.2.3.1.4 Technical Capabilities

The following CCS capabilities are mandatory unless marked optional:

C.2.3.1.4.1 CCS Delivery Methods

The contractor shall provide the following independent service delivery methods for CCS:

1. **Host Based Call Management Service**. The contractor shall provide the necessary components required for CCS Call Management Service at a contractor-provided location. This includes, but is not limited to, hardware, software, inside wiring, and power.
2. **Premises Based Call Management Service**. The contractor shall provide the necessary components required for CCS Call Management Service to be located at an agency-provided location. This includes, but is not limited to, CCS hardware and software. The contractor shall install, configure, and maintain the CCS equipment. The agency will provide the power, inside wiring, and a physical location for the contractor's CCS equipment.
3. **Premises Based Call Answering Service**. The contractor-provided personnel shall perform operations at an agency-provided location. The agency will provide the work space, furniture, workstation hardware, software, and all necessary building utilities required for the contact center.
4. **Host Based Call Answering Service**. The contractor personnel shall be located and perform operations at a contractor-provided location. The contractor shall provide the work space, furniture, workstation hardware, software, and all necessary building utilities for the contact center.

C.2.3.1.4.2 CCS Call Management Service

1. The contractor shall provide the capability for a network call queue (a single queue or multiple queues according to agency needs) to manage the routing and distribution of contacts (calls) from multi-media channels such as voice, email, facsimile, and an agency web site.
2. The intelligent routing and distribution of contacts shall be determined according to the real time operating status of the ordering agency's contact center(s) and its business rules. The agency business rules can be based upon parameters such as media type, real time status of the contact center, caller profile, call content,

and agent skills. The contractor shall provide the capability to prioritize queues and contacts (calls) within a queue.

3. The contractor's CCS shall interoperate with the ordering agency's CCS communications channels such as the web site, e-mail, voice, fax and chat (when applicable).
4. The contractor's CCS shall have the capability to traverse and successfully interoperate with agency firewalls and security layers. The contractor shall verify with the agency that the agency firewall is compatible with the service.
5. The contractor shall support service observation, which provides agency authorized personnel with the capability to monitor the CCS trunks, agents, and agent groups for call quality. The contractor shall provide options for silent monitoring (default) and three-way audio conferencing. Service observation shall be made available for monitoring both local and remote agents and support local and remote observers. Service observation shall be secure and available only to authorized agency-designated individuals.
6. The contractor shall provide the ordering agency with the capability to manage its specific network queue, call routing algorithms, contact center agent profiles, and reports. The CCS shall enable authorized agency designated individuals to perform both real time and scheduled changes. The CCS management system shall provide the following minimum administrative capabilities:
   a) An audit trail and change log history
   b) Authentication with password protection for authorized administrators
   c) Ability to perform scheduled and real-time changes
   d) Ability to view the agency CCS configuration
7. The contractor shall provide reports as required by the OCO.
8. The contractor shall provide the ordering agency with access to graphical, real time reporting of the CCS queue status. The real time reporting shall monitor performance and identify all interactions (voice, email, fax, web and chat) by contact channel and agent status. The reports shall include summaries and totals (where applicable). The real time reporting shall provide the following minimum capabilities:
   a) Number of inbound contacts (calls)
   b) Status of inbound contacts (calls)
   c) Number of contacts (calls) in queue
   d) Length of oldest contact (call) in queue
   e) Average queue time
   f) Number of abandon calls
   g) Agent status and performance statistics

h) Service level information

i) Number of contacts handled by workgroup or skill

9. The contractor shall provide the capability to inform the caller of the queue status including the callers estimated wait time in queue when a queue threshold exceeds an agency defined threshold. This can also include an option for announcing the caller's expected wait time prior to entering the queue. The contractor shall provide agencies with the ability to change recorded announcements.
10. The contractor shall provide the capability to transmit and deliver music on hold (or recordings) to the originating caller. The music on hold source can be contractor or agency provided according to the ordering agency's needs.
11. The contractor shall supply terminal devices (e.g., phones, IP phones, softphones) required for delivery of CCS if requested by the ordering agency. Terminals shall have the capability to support caller ID and an optional name/message display (where applicable).
12. The contractor shall provide the capability to accommodate agency contact center closings (e.g., scheduled holidays, unplanned closings, outside of normal business hours, and closings for maintenance activities) by providing announcements, messages, or re-routing of contacts during the period when the agency contact center is closed.

C.2.3.1.4.3 CCS Call Answering Service

1. The contractor shall provide a CCS Call Answering Service. The contractor shall provide agencies with a contact center operation, which may include network services, technology, personnel, business processes and workflows, training, and reporting to respond to caller inquiries and meet pre-determined performance or customer satisfaction levels.
2. The contractor shall meet the following CCS Call Answering Service requirements:
   a) The contractor shall receive and accurately respond to caller inquiries during established agency operating hours within the agreed-upon KPIs.
   b) The contractor shall manage and accurately respond to caller inquiries received during non-operational hours and holidays according to the ordering agency's needs.
   c) The CCS shall be interoperable with the ordering agencies' required back office systems or databases (if required and as identified by the agency) to deliver the specified customer service functions at the agreed-upon performance levels.
   d) The contractor shall provide resources, processes, and technology to reasonably accommodate inquiries from different types of callers as identified

by the ordering agency. This shall include responding to inquiries from callers that may have foreign language requirements or callers with disabilities including but not limited to speech disabilities, deaf, hard-of-hearing, deaf/blind, or blind (e.g., support TDD/TTY calls).

e) The contractor shall provide a description of its capability to quickly increase capacity in crisis or high-priority situations. The contractor shall quantify its ability to deliver call answer services in terms of capacity, extended operating hours, increased staffing, additional language support and implementation start-up time.

3. The contractor shall provide call answering resources, as needed, in order to meet the requirements specified in the agency service order, according to the descriptions listed in Table C.2.3.1.4.4 below:

C.2.3.1.4.4 CCS Call Answering Resources Table

Role	Description
Basic Call Answering	1. Receive inbound calls and respond to caller inquiries 2. Question callers to obtain full understanding of what information is being requested. 3. Document all customer contacts 4. Follow contact center operational procedures 5. English language proficiency required

C.2.3.1.5 Features

The following CCS features are mandatory unless marked optional.

ID Number	Name of Feature	Description
1	Call Recording and Monitoring	The contractor shall provide digital recording and monitoring of inbound and outgoing multimedia contacts (telephone, email, and web self-service channels) and associated data (agent screen capture) to capture the caller experience. At a minimum, the date, time, duration, caller ID information (if available), dialogue, and identity of the agent handling the call shall be captured and recorded. Archived calls shall be able to be retrieved by date, time, agent, content, contact channel, or identity of the caller. The following minimum capabilities shall be provided: 1. Archive recordings 2. Playback of recording 3. Provide the capability for the recording of an agent to be activated and de-activated on demand. 4. Remote monitoring and playback

ID Number	Name of Feature	Description
		5. Reporting (management and administrative) 6. Programmable scheduled and random call recording 7. Selective recording (based on business rules) 8. Support free seating 9. Total and random recording of all calls 10. Convert call recordings to .wav or mp3 file format The call monitoring system shall also provide the capability for evaluating and scoring calls and performing random call quality reviews.
2	Collaborative Browsing	This contractor shall allow bi-directional sharing of web pages between the contract center agent and the caller. It shall enable a caller to request a co-browse session with a contact center agent. The agent shall have the capability to highlight text and scroll the browser screen to a specific section of a web page. The agent shall have the capability to push a web page to the caller and vice-versa. The contractor shall allow the capability for an agent to transfer control of a collaborative browsing session to another agent and log all collaborative interactions between the agent and caller. The contractor shall state if there are any restrictions or limitations regarding the type of web browser software used by the caller or contact center agent for use with this feature. The contractor shall provide the ability to mask fields and inputs of private/sensitive information.
3	Computer Telephony Integration (CTI)	The contractor shall provide Computer Telephony Integration (CTI) capability to enable transfer of caller information and agency specified data between the contractor and agency specified systems simultaneously with the associated inbound contact channel (call). This feature can be used to support a diverse set of agency applications such as screen pop/splash, intelligent routing, third party call control, keyboard dialing, enhanced reporting, and multi-channel call blending solutions.
4	Customer Contact Application	The contractor shall provide an application to track, document, and manage the CCS customer contacts across multiple contact channels. The customer contact application shall contain the following minimum capabilities: 1. Record caller contact information 2. Record caller account information 3. Record caller contact history and status of inquiry 4. Record nature of the inquiry 5. Record date and time of the contact 6. Record call disposition 7. Record agent handling the inquiry 8. Assign & escalate inquiries according to business rules

ID Number	Name of Feature	Description
		9. Assign a unique case or record number to each inquiry The customer contact application shall also provide the capability to create and provide scripted responses for the contact center agents. The contact system shall also provide summary and detailed management reports.
5	E-mail Response Management	The contractor shall provide E-mail Response Management (ERM) that shall assign a tracking ID to each email and route e-mail communication according to agency specified business rules. The ERM shall provide the following minimum capabilities: 1. Auto response 2. Automatic acknowledgement 3. Email classification and prioritization 4. Email routing based upon business rules 5. Filtering capability 6. Content analysis and knowledge base for suggested and personalized responses 7. Management reports 8. Multiple language support (English and Spanish) 9. Real time exception reports The ERM shall be compatible with the ordering agency's e-mail application.
6	Interactive Voice Response (IVR)	The contractor shall provide an interactive voice response application that allows callers to be provided with information based upon input from (a) telephone DTMF key pad entries or via (b) speech recognition. The minimum capabilities are listed below: 1. Select pre-recorded announcement messages with the capability for announcements and provide the ability for a caller to opt out during an announcement to a predefined termination. Such announcements shall always be played from the beginning for each caller and provide the capability to be recorded in (a) U.S. English, (b) Spanish (American) and (c) other foreign languages after obtaining ordering agency script approval. 2. Leave caller information via telephone DTMF keypad signal or speech (e.g., name, address, account information, etc.). 3. A means for the ordering agency to retrieve caller-entered DTMF or speech messages. 4. For transcription of caller information, the contractor shall provide (a) transmission of the recorded voice files and DTMF data for each call to the agency and (b) a report of caller responses that transcribes the caller-provided information for the ordering agency based upon the agency's needs and transmits it to

ID Number	Name of Feature	Description
		the agency. The contractor shall provide transcription reports from English- and Spanish-speaking callers. 5. Query a database that delivers agency-provided information to the caller. The database may be housed in the (a) ordering agency or, at the ordering agency's discretion, (b) housed in a contractor location and updated by the ordering agency. Provide a default routing or message (agency option) if the database is unavailable. 6. Provide a capability to allow callers to hear and verify their names and addresses in an agency-provided name and address database after the caller has entered his or her telephone number via DTMF, or based on the caller's ANI. (Text to Speech). 7. Support speech recognition as a valid caller input. The contractor shall support at a minimum, all spoken numeric digits as well as "yes" and "no." English and Spanish language callers shall be supported. The contractor shall be able to accept and process at a minimum 95 percent of the above speech responses. The speech responses which are not accepted shall be routed to default location designated by the ordering agency. 8. Provide the capability to perform surveys (via DTMF or speech) to IVR callers. The surveys can be provided to all or a random percentage of callers according to agency needs. Survey results shall be provided electronically to the ordering agency. 9. Provide a facsimile "fax back" capability (Fax or equivalent) that shall permit callers to retrieve agency-specific documents or forms. The contractor shall fax back the request documents within one hour of the initial call and retry a minimum of 13 attempts over a six hour interval in order to complete the request. Fax transmittal shall include an option for a cover sheet (standard or customized). 10. At the agency's option, the caller's IVR selection(s) information shall be transferred to the agency. 11. The contractor's IVR capacity must be configured such that the application answers a call within 3 ring cycles for 99 % of the offered call volume (measured on an hourly basis). 12. Features equivalent to the above shall be available to individuals who are hearing impaired or have speech disabilities via electronic means in Baudot and ASCII/TTY code formats. These electronic form lines need not be voice feature enabled. 13. The contractor shall provide summary reporting that at a minimum provides information on the caller, average call duration, caller opt out (transfer) and

ID Number	Name of Feature	Description
		disposition of the calls within the IVR application on a daily, weekly and monthly basis. 14. The contractor shall make available any IVR reports that are available with its equivalent commercial offerings
7	IVR - Agency Based Database (Host Connect)	The contractor shall provide the ability to route calls or provide information based upon a database query(s) of information provided by a database located at the ordering agency premises. The query(s) could be to single, redundant, or multiple databases depending upon agency specifications and the complexity of the application. The contractor shall implement and provide the appropriate interface and connectivity for the contractor's IVR application to successfully query and access the ordering agency's database(s). The IVR caller shall have the capability to retrieve, review, and modify information located on the agency based database based upon the ordering agency's needs. The agency database(s) can be a (a) mainframe or (b) server based relational database. If the database does not respond to the network query within 250 milliseconds, an agency defined default routing plan shall be used.
8	Reserved	
9	IVR - Speech Recognition	The contractor shall provide natural speech recognition for IVR applications with the ability, at a minimum, to recognize spoken vocabulary, digits, zip codes, credit card numbers, credit card expiration date, account numbers, alpha numeric numbers. At a minimum the contractor shall provide natural speech recognition capabilities and vocabularies for both English (American) and Spanish (American) dialects. The minimum accuracy threshold for speech recognition shall be at least 95%.
10	Language Interpretation Service	The contractor shall provide telephone language interpretation services. The service should be available, on demand, for three way conferencing with the contact center agent and foreign language caller to provide interpretation between the caller's foreign language and English and vice versa. This feature shall have the following minimum capabilities: 1. Available 24x7 2. Accessible via a toll free number 3. Identify the foreign language of the caller 4. Provide an appropriate interpreter within one minute of the request 5. Provide management reports identifying the date, time, duration, interpreter, and identity of the agent requesting the service.

ID Number	Name of Feature	Description
		The contractor shall propose and provide a list of the foreign languages available for interpretation. Spanish is a mandatory language.
11	Outbound Dialer	The contractor shall provide the capability for automated outbound dialing. The dialer service shall have the capability to support either centralized or distributed contact center environments according to the ordering agency's needs. The dialer shall have the following minimum capabilities: 1. Automatically initiate domestic and non-domestic outbound calls 2. Call conferencing and call transfer capability 3. Predictive dialing - capture real-time statistics from the call queue and automatically adjusting the outbound dialing frequency according to agency defined service level parameters 4. Preview dialing - allow agents to preview the customer record before an outbound call is initiated and provide an option for the agent to cancel the call 5. Receive and manage inbound calls 6. Support agent blending. The integration of outbound and inbound call handling to determine how to best use agent resources. (agents can handle both outbound and inbound calls) 7. Support service observation 8. Reporting – Provide comprehensive historical, real time management, and exception reports.
12	Text Chat (Web Chat)	The contractor shall provide the ability to enable the contact center agents to engage in real time text chat with callers directed from its web site. The text chat shall provide the following minimum capabilities: 1. Archive text chat sessions (create transcripts) 2. Allow agents to manage multiple text chat sessions 3. Allow file transfers 4. View the active web page the text chat caller is on 5. Provide a log of text chat sessions 6. Provide an automatic spell check and grammar check option that is enabled when typing in active session. 7. Supervisor chat monitoring
13	Web Call Back	The contractor shall provide the capability for a customer to request a call back by filling out a form on the agency's web site. The call back algorithm shall be based upon the availability of a contact center agent. The call back request shall be automatically distributed to the most appropriate agent based upon availability of an agent (within agency operating hours).
14	Web Call Through	The contractor shall provide the capability to enable customers browsing the agency's web site the ability to

ID Number	Name of Feature	Description
		call through (e.g. “click to talk”) and simultaneously have a voice conversation with a contact center agent.
15	Workforce Management	The contractor shall provide a workforce management (WFM) system that automates forecasting and scheduling calculations based upon real time and historical contact center data. The WFM shall enable agencies to effectively schedule resources, accurately forecast call volumes and analyze/review performance statistics for single or multiple sites and blended applications. The workforce management system should provide the following minimum capabilities: 1. Forecast staffing needs including agent skills, skill levels and shifts. 2. Forecast contact volumes and workload - overall call volume and by contact channel. 3. Provide agent scheduling and create optimized agent schedules by shift and skill.
16	Virtual Queue	The contractor shall provide a capability whereby callers can choose to remain waiting on-line for an attendant or receive a call back in turn.

C.2.3.1.6 Interfaces

CCS is an application layer service which uses underlying network service(s) to deliver customer service capabilities. Where applicable, refer to the interface requirement sections below:

1. Section C.2.2 Voice Service
2. Section C.2.4 Colocated Hosting Service

C.2.3.1.7 Performance Metrics

The performance levels and AQL of KPIs for CCS are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
	Critical	99.9%	≥ 99.9%	
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 2

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Availability is measured and calculated as a percentage of the total reporting interval time that CCS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section G.8.2 for the definitions and measurement guidelines.

C.2.4 Colocated Hosting Service

There may be requirements for the contractor to provide facilities for a data center that will be populated by GFP, such as servers, routers and load balancers.

C.2.4.1 Functional Definition

Colocated Hosting Service (CHS) shall provide a secure location with cage and racks and include site surveillance. This service also provides external traffic access as required; Internet and other dedicated connection (e.g., PLS and ETS) speeds, space requirements, maintenance support and operational support will be specified in TOs.

The contractor shall provide the government and its representatives with 24x7 access to leased space and GFP in the co-location facility. The co-location facility shall support the following capabilities:

1. Redundant and high-availability power to GFP.
2. Redundant Uninterruptible Power Supplies (UPS). UPS systems shall receive power both from commercial power feeders and alternate power sources.
3. A Very Early Smoke Detection Apparatus (VESDA) system shall be provided for fire detection.
4. A fire suppression system shall be provided. Acceptable systems include (but are not limited to) multi-zone, pre-action, dry pipe systems.
5. Redundant cooling systems.

C.2.4.2 Standards

CHS shall comply with the following standards:

1. TIA-942 Telecommunications Infrastructure Standard for Data Centers (as updated)
2. NIST SP800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations
3. ICD 705, 26 May 2010, Sensitive Compartmented Information Facilities (as required)

C.2.4.3 Connectivity

CHS shall provide external connectivity as required in accordance with the TO.

C.2.4.4 Technical Capabilities

CHS requires the following mandatory capabilities:

1. At the contractor's facility, the contractor shall be responsible for the following, as required:
   a) Assuming responsibility for all damage or injury to persons or property occasioned through the use, maintenance, management, and operation of the contractor's facilities, GFP, or other equipment by, or by the action of, the contractor or contractor's employees and agents. The government shall in no event be liable or responsible for damage or injury to any person or property occasioned through the use, maintenance, management, or operation of any facility, GFP, or other equipment by, or by the action of, the contractor or the contractor's employees and agents in performing under this contract, and the Government shall be indemnified against claims for damage or injury in such cases.
   b) Completing any necessary pre-delivery preparations for the delivery site, site security, or storage facilities to temporarily or permanently accommodate the GFP in a safe and secure manner.
   c) Relocating GFP from initial receiving points or temporary storage facilities to the final contractor facility and installation site.
   d) Preparing the final installation site including the provisioning of necessary physical space, environmental systems, and network connectivity, including but not limited to: Internet working connections, fire suppression, HVAC, power, lighting, water, sewer, telephone and communications, physical security systems, network security systems, disaster resistance and recovery systems, cages, racks, and UPS, emergency power systems, all on a 24x7 basis, unless otherwise mutually agreed upon and specified.

e) Facilitating GFP setup, including assembling, loading, configuring, testing, and (at end of life) crating and packing GFP for return. Determinations of inter-compatibility and inter-operability shall be conducted by the contractor as soon as practical after delivery and setup.

f) Providing contractor personnel with all required national citizenship, security clearances, training, and technical certifications to receive, use, maintain, manage, operate, package, transport, or ship sensitive and secure GFP.

2. Authorized government personnel and third-parties shall have access to GFP at specified times, in specified locations, as mutually agreed upon between the government and the contractor. Government personnel shall conform to the contractor's Acceptable Use Policy (AUP) in effect at the specified contractor facility, except where the AUP conflicts with government policy, or other government executive orders, regulations or laws.
3. The contractor shall provide a service management capability such that user can remotely monitor facility and equipment status in real-time.
4. The service management capability shall present alarms to the user in real-time for facility and communication failures.
5. The service management capability shall continuously update and present to the user the status of power for each rack, cooling, environment temperature, entry/exit logs, smoke detection, and connectivity.

C.2.4.5 Features

The contractor may be required to provide CHS in an Intelligence Community Directive (ICD) 705 Sensitive Compartmented Information Facility (SCIF). The size and other characteristics of a SCIF will be provided in the TO.

C.2.4.5.1 Performance Metrics

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Internet Availability	Critical	99.99%	≥ 99.99%	See Note 1
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 2

Notes:

1. Availability is measured and calculated as a percentage of the total reporting interval time that CCS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section G.8.2 for the definitions and measurement guidelines.

C.2.5 Cloud Service

NIST SP 800-145 defines cloud services as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). All cloud services offered shall be FedRAMP certified. The contractor shall support the five essential characteristics and four deployment models of cloud services defined in NIST SP 800-145 and listed below.

Essential characteristics:

1. On Demand Self-Service – ability to select and provision services as needed
2. Broad Network Access – universal access to thin or thick client platforms such as mobile devices, laptops, and PDAs
3. Location Independent Resource Pooling – computing resources are shared, serving multiple consumers
4. Rapid Elasticity – ability to immediately scale up or down based on user needs and peak demands
5. Measured Service – ability to pay only for what is used

Deployment Models:

1. Private cloud – generally controlled, managed, and hosted by a single organization
2. Community cloud – same as Private cloud except that the cloud is shared by multiple organizations (e.g., federal agencies or sub-agencies) with similar security and performance goals
3. Public cloud – different users share infrastructure and receive a standardized, yet highly scalable, type of capacity
4. Hybrid cloud – combination of at least one Private cloud and one Public cloud connected to allow programs and data to be easily shared. This allows an organization, for example, the ability to burst fluctuating workloads into the public cloud when necessary.

The deployment of cloud services in the Federal Government is mandated by the OMB's "Cloud First" policy for any federal IT acquisition, the Federal Cloud Computing Initiative (FCCI) by the Federal CIO Council for government cloud computing framework

and requirements, and FedRAMP for a unified risk management framework for cloud computing.

In accordance with the NIST and Federal mandates and requirements, the contractor shall support cloud services (IaaS, PaaS, and SaaS in any combination) as described in the following sub-sections.

C.2.5.1 Infrastructure as a Service

C.2.5.1.1 Service Description

The contractor shall provide a solution for provisioning required computing and networking resources and supporting the FedRAMP and TIC overlay requirements.

IaaS shall be composed of the following subservices: 1) Private Cloud IaaS and 2) Data Center Augmentation with Common IT Service Management (ITSM). These subservices are described in the following subsections.

C.2.5.1.1.1 Functional Definition

The Private Cloud IaaS subservice shall offer a private cloud IaaS solution that includes virtual machines, storage, and server hosting. The cloud platform provides necessary network infrastructure (e.g., LAN, load balancer, and firewall), security components, storage backup, continuity of operation, and disaster recovery services. The private cloud may be either an “air-gapped Private Cloud” where the cloud platform is based on physical infrastructure dedicated to the customer agency, or a “virtual-gapped Community Cloud” where the cloud platform physical infrastructure is shared by two or more agencies and the allocated virtual resources are separated by an agency-specific security envelope/perimeter.

The Data Center Augmentation with Common ITSM subservice shall enable augmentation of already-virtualized agency premises data center resources with dynamically expandable and contractible virtualized cloud-based resources. This service includes a common IT management framework for agency data center resources and cloud resources. The common ITSM framework for data center resources will allow data center managers to follow the same processes for managing the additional cloud resources that they use to manage their data center resources.

C.2.5.1.1.2 Standards

IaaS shall comply with the following standards:

1. NIST:
   a) NIST SP 800-145 "The NIST Definition of Cloud Computing," September 2011

b) NIST SP 500-292 "NIST Cloud Computing Reference Architecture," September 2011
c) NIST SP 800-53 (rev.4) "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013
d) NIST SP 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," April 2010
e) NIST SP 800-46 (rev.1) “Guide to Enterprise Telework and Remote Access Security”
f) NIST SP 800-171 “Protecting Controlled Unclassified Information in the Nonfederal Information Systems and Organizations,” June 2015

2. ITIL: ITILv3
3. SNMP: SNMPv3
4. FedRAMP TIC Overlay; see https://www.fedramp.gov/files/2015/04/Description-FT-Overlay.docx
5. OMB M-06-16 "Protection of Sensitive Agency Information," 23 June 2006
6. ISO 17203 “Open Virtualization Format Specification”
7. FIPS 140-2, Security Requirements for Cryptographic Modules
8. FIPS 197, Advanced Encryption Standard
9. DOD STD-5015.2 V3, Electronic Records Management Software Applications Design Criteria Standard
10. NARA Bulletin 2008-05, July 31, 2008, Guidance concerning the use of e-mail archiving applications to store e-mail
11. NARA Bulletin 2010-05, September 08, 2010, Guidance on Managing Records in Cloud Computing Environments

C.2.5.1.1.3 Connectivity

Network connectivity from agency sites to the contractor’s cloud services shall be supported through communications services offered through this contract as appropriate.

C.2.5.1.1.4 Technical Capabilities

C.2.5.1.1.4.1 Technical Capabilities of Private Cloud

The contract shall support the basic capabilities for Private Cloud IaaS defined in NIST SP 800-145 as specified in the TO. These capabilities are mandatory unless marked optional:

1. Access to agency data in data centers shall comply with National Policy as defined in C.1.8.8 including agency sites and remote locations.

2. Cloud Data Center Security:
   a) Provide secure connectivity among contractor's data centers for elasticity (expansion and contraction) of computing resources
   b) Secure connectivity to contractor's data center from agency sites
   c) Provide additional compliance and certification requirements as specified in the TO
3. Agency Cloud Service Security
   a) Create and maintain a security perimeter around an agency's data and VMs
   b) Data-at-rest encryption in accordance with FIPS 197
4. Virtualized elastic computing infrastructure:
   a) Virtual Machines (VMs)
   b) Network Storage
5. Server Hosting
   a) Private-facing Internal Web Hosting
   b) Public-facing External Web Hosting
6. Backup and Restore agency data
7. On-demand self-service IaaS provisioning, configuration management, topology management, security management, activation and deactivation via portal scripting language or API with role based access control for portal login which is OMB M-11-11 compliant
8. Visibility into usage of measured/metered (usage-based) service.
9. Allow users to have VMs with their own private IP address blocks.
10. Support bulk import and export of VM per ISO 17203.
11. Allow users access to log events such as resource provisioning and de-provisioning, VM start and stop, and account changes, for at least 60 days.
12. (Optional) Allow users to place metadata tags on provisioned resources and to run reports based on them, which is useful for internal showback or chargeback.
13. Support cost control measures such as quotas (limits on what a user can provision) and leases (time-limited provisioning of resources).
14. Support with 24x7 customer service, via phone, email and chat.
15. The agency retains exclusive ownership over all of its data in the cloud. The contractor shall provide tools to allow the client agency to fully retrieve its data in the original or a mutually agreed-upon format.
16. Cloud resources, particularly the data at rest, must be located within the U.S. or the jurisdiction identified in the TO to allow electronic discovery (eDiscovery) of identification, collection, processing, forensic analysis, auditing, and production of

Electronically Stored Information (ESI) required in the discovery phase of litigation. This shall also include government access to the contractor's cloud data center facilities, installations, technical capabilities, operations, documentation, records, and databases if required. See Section H.33 for additional eDiscovery requirements.

17. The contractor shall provide Disaster Recovery (DR) and Continuity of Operations (COOP) per agency-specific requirements in the TO.

C.2.5.1.1.4.2 Technical Capabilities of Data Center Augmentation with Common Information Technology Service Management

The contractor shall support the following technical capabilities for Data Center Augmentation with Common ITSM. The following capabilities are mandatory unless marked optional:

1. Ability to manage both cloud virtual resources and the agency data center's virtual resources with interoperable monitoring and control capabilities.
2. The contractor's management platform shall include a visual indicator of which resources are in the cloud and which are premises resources.
3. (Optional) Ability to integrate with agency's data center management platform.

C.2.5.1.2 Features

The following features are mandatory unless marked optional:

1. (Optional) "Bare metal" physical servers: Ability to have "bare metal" physical servers on a dynamic basis with provisioning times of two hours or less. This capability may be required for (a) a large-scale database requiring an incremental storage capacity, or (b) specialized network equipment that may not be available in the cloud, or (c) software that cannot be licensed on virtualized servers, or (d) legacy equipment that cannot be virtualized, or (e) agencies that plan to move into collocation first and then gradually migrate into the provider's cloud.
2. Data management and analytics: This capability shall complement and extend log management and analysis services and other data center management services, per agency-specific requirements in the TO.

C.2.5.1.3 Interfaces

The contractor shall support the interfaces identified in the TO.

C.2.5.1.4 Performance Metrics

The performance levels and AQL of KPIs for the contractor's IaaS cloud service are defined below. In addition, the contractor shall meet service level objectives for performance, privacy, security and support as specified in the TO.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability (IaaS cloud service)	Routine	99.95%	≥ 99.95%	See Note 1
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. IaaS cloud service Infrastructure availability is calculated as a percentage of the total reporting interval time that the IaaS infrastructure is operationally available to the agency. Availability is computed by the standard formula:

$$Av(IaaS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

The scheduled maintenance windows are excluded from the availability calculation.

C.2.5.2 Platform as a Service

C.2.5.2.1 Service Description

C.2.5.2.1.1 Functional Definition

PaaS provides the capability for the user to deploy and employ applications using software tools supported by the cloud provider.

C.2.5.2.1.2 Standards

Same as specified for IaaS. See Section C.2.5.1.1.2 for details.

C.2.5.2.1.3 Connectivity

Same as specified for IaaS. See Section C.2.5.1.1.3 for details.

C.2.5.2.1.4 Technical Capabilities

The contractor shall provide the following PaaS capabilities including, but not limited to:

1. Access to agency data in data centers shall comply with National Policy as defined in C.1.8.8 including agency sites and remote locations.
2. Developer Tools:
   a) Integrated Development Environment (IDE) Suite
   b) Application Server
   c) Utilities/Libraries
3. Database Systems (DBMS/RDMS)
4. Big Data Solution Platform
5. Directory, based on, but not limited to, LDAP/X.500 based implementations, to support directory schemas, defined as object classes, attributes, name bindings, and knowledge (namespaces)
6. Testing Tools:
   a) Application Test Tools
   b) Web Test Tools
   c) Workflow Tools

The agency retains exclusive ownership over all of its data in the cloud. The contractor shall provide tools to allow the client agency to fully access PaaS-related data from the cloud in a usable format as needed.

C.2.5.2.2 Features

None.

C.2.5.2.3 Interfaces

The contractor shall support the interfaces identified in the TO.

C.2.5.2.4 Performance Metrics

The contractor shall meet PaaS cloud service KPIs. See Section C.2.5.1.4 for details.

In addition, the contractor shall meet service level objectives for performance, privacy, security and support as specified in the TO.

C.2.5.3 Software as a Service

C.2.5.3.1 Service Description

C.2.5.3.1.1 Functional Definition

Software as a Service (SaaS) allows software and applications to be hosted in the cloud and accessed by users via, for example, agency intranet.

C.2.5.3.1.2 Standards

Same as specified for IaaS. See Section C.2.5.1.1.2 for details.

C.2.5.3.1.3 Connectivity

Same as specified for IaaS. See Section C.2.5.1.1.3 for details.

C.2.5.3.1.4 Technical Capabilities

The contractor shall provide the following SaaS capabilities including, but not limited to:

1. Access to agency data in data centers shall comply with National Policy as defined in C.1.8.8 including agency sites and remote locations.
2. Customer Relationship Management (CRM) tools
3. Enterprise Resource Planning (ERP) tools
4. Human Capital Management (HCM) tools
5. Desktop applications
6. Office automation tools
7. Security tools
8. Others as defined in the TO

The agency retains exclusive ownership over all of its data in the cloud. The contractor shall provide tools to allow the client agency to fully access SaaS-related data from the cloud in usable format as needed.

C.2.5.3.2 Features

None.

C.2.5.3.3 Interfaces

The contractor shall provide the following UNIs:

1. The contractor shall support the interfaces identified in the TO.
2. Platform-specific API or client software to connect to the cloud SaaS platform.

C.2.5.3.4 Performance Metrics

The contractor shall comply with the following performance metrics:

1. Same as specified for IaaS. See Section C.2.5.1.4 for details.
2. Most current software release with all the patches applied or as specified in the TO.

C.2.5.4 Content Delivery Network Service

C.2.5.4.1 Service Description

Content Delivery Network Service (CDNS) delivers agency content to Web browsers worldwide. The CDNS provider incorporates equipment and algorithms to cache content on geographically dispersed servers on the Internet. When a request is made from a particular location for specific content, the server that can most rapidly and efficiently provide the content is dynamically identified.

C.2.5.4.1.1 Functional Definition

A Content Delivery Network (CDN) consists of a collection of surrogate servers that attempt to offload work from origin servers by delivering content on their behalf. The servers belonging to a CDNS may be located at the same site as the origin server, or at different locations around the network, with some or all of the origin server's content cached or replicated among the CDNS servers. For each request, the CDNS attempts to locate a CDN server close to the client agency to serve the request, where "close" could include geographical, topological, or latency considerations.

CDNS addresses the following technical and operational issues:

- Latency – the delay in delivering Web content to the end-user
- Scalability – Web services automatically scale up as end-user requests increase
- Reliability – content is always available and its integrity is assured (i.e., has not been altered by third parties including hackers)
- Flash crowd control – i.e., effectively meeting demand during periods of unexpected high usage

C.2.5.4.1.2 Standards

CDNS shall comply with the following standards:

1. Hyper Text Transfer Protocol (HTTP)
2. IETF – Request for Comments
3. Transport Layer Security (TLS)

The contractor shall comply with new versions, amendments, and modifications made to the above listed documents/standards.

C.2.5.4.1.3 Connectivity

CDNS shall connect to and interoperate with the following:

1. Internet for content distribution to public
2. IP network (agency-owned or contractor-provided) for loading and administration of web server by the agency

C.2.5.4.1.4 Technical Capabilities

The following CDNS capabilities are mandatory unless marked optional:

1. Content Distribution:
   a) Static Content Download Service:
      i. This service provides fast, secure, and reliable download of content including text, video and music. Such content will likely be stored on CDNS servers that are deployed globally.
   b) Real-time Streaming (Webcasting):
      i. The contractor shall deliver streams in real time (the CDNS shall encode the signal when sent in raw signal format by the content provider).
      ii. Real-time streaming content may include (but not be limited to) RealNetworks Real Media, Microsoft Windows Media, and Apple QuickTime.
   c) On-demand Streaming:
      i. The contractor shall host (i.e., provide storage) and deliver streams on demand or when requested by end-users (the CDNS shall encode the signal when sent in raw signal format by the content provider).
      ii. On-demand streaming content may include (but not be limited to) RealNetworks Real Media, Microsoft Windows Media, and Apple QuickTime.
2. Site Monitoring/ Origin Server Performance Measurements:
   a) The contractor shall perform continuous monitoring to ensure performance and quality of service. Measurements shall include:
      i. Availability
      ii. Latency
      iii. FTP Load

iv. CPU Load
v. Memory Usage
vi. TLS Service Load
vii. HTTP Port Service Load
viii. HTTP Connections Queue Statistics

b) The contractor shall provide statistics via a performance dashboard – a secure, Web-based portal accessible 24x7 by agency clients. The performance dashboard shall be consistent with commercial best practice.

C.2.5.4.2 Features

The following features are mandatory unless marked optional:

1. Failover Service: This service monitors single-location web sites (maintained by agencies or third parties under contract to agencies) and redirects traffic to a CDNS in the event of failure. This service shall ensure that end-users do not experience delays, site inaccessibility, or error messages.
2. (Optional) Redirection and Distribution Service (Global Load Balancing): When users type in a web site address or Universal Resource Locator (URL), they rely on Domain Name System (DNS) servers to direct them through the Internet and connect them to the specified Web server. Redirection and distribution services ensure that all Web requests are directed to the closest, most available cache server. Typically a set of surrogate servers is provisioned to cache content for the content provider's origin server, enabling requests to bypass congested areas. Redirection and Distribution Services may employ any proven technique(s) including, but not limited to:
   a) DNS Redirection
   b) URL Rewriting
   c) Layer-4 Switching
   d) Layer-7 Switching
   e) HTTP Redirection

C.2.5.4.3 Interfaces

The contractor shall provide the following UNIs:

1. For access via Internet: Hyper Text Transfer Protocol (HTTP).
2. For agency connectivity to the CDNS server: UNIs as defined in VPN Service (VPNS). See Section C.2.1.1.1 for details.

C.2.5.4.4 Performance Metrics

The contractor shall comply with AQL of KPIs for CDNS as defined in Section C.2.5.4.4.1 below.

C.2.5.4.4.1 Performance Metrics for CDNS

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability (CDNS network)	Routine	99.99 %	99.99 %	See Note 1
GOS (Time to refresh content)	Routine	5 minutes	≤ 5 minutes	
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. CDNS availability is calculated as a percentage of the total reporting interval time that the CDNS is operationally available to the agency. Availability is computed by the standard formula:

$$Av(CDNS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

C.2.6 Wireless Service

C.2.6.1 Service Description

C.2.6.1.1 Functional Definition

Wireless Service (MWS) is a wireless transmission service for mobile terminals. The contractor provides the wireless network.

The services and bandwidth provided depend on the characteristics of the mobile terminals and the technology used in the contractor's wireless network and service platforms, ranging from 2nd generation (2G) to 2.5G/3G to 4G LTE wireless.

Short Messaging Services (SMS), a feature of MWS, provides the capability to send and receive text messages. The text can comprise of any alphanumeric characters; each short message may be up to 160 characters in length.

Multimedia Messaging Service (MMS), a feature of MWS, provides the capability to send and receive multimedia, such as pictures, streaming video, sound, and graphics.

C.2.6.1.2 Standards

MWS shall comply with the following standards:

1. 2.5G [based on General Packet Radio Service (GPRS) or Code Division Multiple Access (CDMA-2000 – 1xRTT)]:
   a) ETSI GSM-MAP
   b) TIA IS-41
2. 3G [based on CDMA] ITU-RTT IMT-2000:
   a) European ETSI/GSM Wideband CDMA (WCDMA) (also known as Universal Mobile Telecommunications System (UMTS))
   b) US CDMA Development Group (CDG) CDMA-2000 Evolution Data Optimized (EV-DO)
3. 4G [based on 3GPP Long Term Evolution (LTE)]:
   a) ETSI TR25.913
4. Wireless Application Protocol (WAP):
   a) WAP Forum (Wireless Application Protocol (WAP 1.1 and 2.0) via WAP Gateway)
   b) IP Mobility Support, IETF RFC 2002
5. 3G Security:
   a) 3GPP TS 21.133
   b) NIST FIPS Publication 140-2
6. Short Messaging Service (SMS)
   a) 3GPP TS 03.40
   b) GSM 03.41
7. Multimedia Messaging Service (MMS):
   a) 3GPP TS 23.140
   b) Open Mobile Alliance
8. 5G Future (according to Next Generation Mobile Networks Alliance group) – draft standards are under study, but the service is expected to roll out by 2020:
   a) Will efficiently support the Internet of Things, broadcast-like services, and lifeline communications in times of natural disaster, as well as novel applications such as mission critical control or traffic safety, requiring reduced latency and enhanced reliability.
   b) May be based on new technologies such as mesh networking and/or beam-division multiple access and relays with group cooperation, whereby devices

communicate with each other directly rather than relying on network operators' base stations.

9. The contractor shall comply with new versions, amendments, and modifications made to the above-listed documents/standards including beyond 4G.

C.2.6.1.3 Connectivity

MWS shall connect to and interoperate with the following:

1. The Public Switched Telephone Network (PSTN) and the worldwide dialing plan per ITU Recommendation E.164
2. Originate and terminate calls to users of commercial satellite-based services
3. The Internet
4. Agency mobile terminals, such as, but not limited to cellular phones, smartphones, wireless-enabled Notebook and Laptop PCs, and PDAs

C.2.6.1.4 Technical Capabilities

The following MWS capabilities are mandatory unless marked optional:

1. MWS shall have the capability to originate and receive voice calls from mobile phones, fixed wireline networks, and satellite-based networks.
2. The contractor shall provide mobile devices (smartphones and cellular phone) as required (see Section C.2.10 Service Related Equipment) supporting the following capabilities:
   a) Cellular Phones:
      i. Built-in available features
      ii. Wireless broadband devices (e.g., mobile Wi-Fi hotspots, MiFi - wireless router that acts as a mobile Wi-Fi hotspot)
      iii. Secure voice communications with FIPS-compliant encryption (as available)
   b) Smartphones:
      i. Built-in available features
      ii. Email
      iii. Web browser
      iv. Personal Information Management (PIM), including contact and calendar information and documents/notes
      v. Ability to sync with leading email, contact/address, and calendar platforms
      vi. Vibrate alert to emails and text messages
      vii. Ring alert to emails and text messages
      viii. Ability to transfer photos/pictures directly to computer

ix. Remote kill (as available)
x. Remote wipe (as available)
xi. Ability to disable audio, video, and all recording functionality (as available)
xii. Transmit and receive data (e.g., run an agency specific app) while conducting a voice session (as available)

3. The contractor shall offer the following MWS plans and plan aspects for GFP and user-owned devices.
   a) Voice Service Plans shall include voice calling and text messaging (SMS).
   b) Data Add-On Service Plans shall include data added to voice service plans. Data may include email, Internet access, video, Multimedia Messaging Service (MMS), and other data.
   c) Data only Service Plans shall include emails, Internet access, video, MMS, and other data transport not combined with voice service plans.
   d) (Optional) Machine-to-machine (M2M) – M2M and telemetry products shall provide wireless connectivity to machines, vehicles, or assets
   e) Mobility applications for mobile device management (see Section C.2.8.6 Managed Mobility Service).
   f) Mobile Roaming Plans. Domestic and non-domestic mobile roaming plans shall cover voice calls, messaging, multimedia, and data.
   g) Pooling of domestic data. Pooling of domestic data (gigabytes) within the same billing account at a level specified by the ordering entity (e.g., an entire agency or multiple sub-bureaus within an agency).
4. The contractor shall comply with Wireless Enhanced 911 (E911) Rules including Phases I and II as stipulated by the Federal Communications Commission. Refer to http://www.fcc.gov/911/enhanced/.

C.2.6.2 Features

The following features are mandatory unless marked optional:

1. Wireless Priority Services (WPS). WPS allows authorized National Security and Emergency Preparedness (NS/EP) personnel to gain access to the next available wireless radio channel in order to initiate calls during an emergency when channels may be congested. WPS is invoked by dialing *272 prior to the destination number on wireless terminals that have subscribed to WPS. Refer to http:/wps.ncs.gov/. Also see Section G.11.4.2, for NS/EP requirements.
2. Directory Assistance with Call Completion. This feature allows the user to obtain at least two look-up phone numbers and connect to one of them.
3. Domestic to Non-Domestic Calling. This feature allows a user to make non-domestic calls.

4. (Optional) International Mobile Roaming. This feature allows a user to roam internationally with wireless Internet connectivity and communications capability.
5. Personal Hotspot. This feature enables a wireless device to be used as a hotspot to connect another device to the Internet or to a private network.
6. Indoor cellular system (Femtocells and Microcells) installation to allow and/or improve indoor wireless operation.
7. (Optional) Push to Talk with Group Talk enables users to connect directly with other users by pressing a button on their wireless terminals. The service shall indicate via an icon on the handset whether a user on their calling list is available. Business colleagues or work teams shall be able to set up and manage group calling lists. This capability shall support groups of up to 10 participants. Users can create up to 50 group lists and store 100 individual contacts.

C.2.6.3 Interfaces

The contractor shall support the following interfaces for the provisioning of MWS at the SDP, as defined in Section C.2.6.3.1.

C.2.6.3.1 Wireless Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
1	Air Link: (Std: GSM and IS-136 TDMA)	Up to 116 Kbps	1. Transparent 2. IP v4 3. IP v6
2	Air Link: (Std: CDMA 1xRTT)	Up to 144 Kbps	1. Transparent 2. IP v4 3. IP v6
3	Air link: (Std: 3G WCDMA)	Up to 384 Kbps	1. Transparent 2. IP v4 3. IP v6
4	Air Link: (Std: CDMA EVDO)	Up to 500 Kbps	1. Transparent 2. IP v4 3. IP v6
5	Air Link: (Std: WCDMA-HSDPA) [Optional]	Up to 14.4 Mbps	1. Transparent 2. IP v4 3. IP v6
6	Air Link: (Std: 4G LTE)	Up to 100 Mbps (maximum 300 Mbps)	1. ITU 3GPP (TR25.913) 2. IP v4 3. IP v6

C.2.6.4 Performance Metrics

The contractor shall comply with AQL of KPIs for MWS as defined in Section C.2.6.4.1 below.

C.2.6.4.1 Performance Metrics for Wireless Service

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Notes 1 and 2
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. MWS availability is calculated based on availability of access to the contractor's network from the contractor's cell site.
2. Radio access network performance is likely to vary depending on location (e.g., urban, suburban, or rural), as well as the technical specifications and capabilities of the deployed infrastructure, such as the radio access equipment.

C.2.7 Commercial Satellite Communications Service

C.2.7.1 Service Description

C.2.7.1.1 Functional Definition

The contractor shall provide mobile or fixed commercial satellite communications (COMSATCOM) services to include, but not be limited to: satellite bandwidth, satellite service plans, contractor provided earth terminals, radio frequency equipment, satellite phones, interfaces and support services. Specific services will be identified in TOs.

COMSATCOM shall be provided in any commercially available communications satellite frequency band to include, but not limited to, S-, C-, L-, X-, Ku-, Ka- and UHF bands.

Commercial Mobile Satellite Service (CMSS) delivers voice, data and Internet services to land-based, maritime, or aeronautical users using one- or two-way communications via satellite. The service provides an end-to-end connection between CMSS users, or between CMSS and wireline and wireless users via the contractor's network and gateway(s).

Commercial Fixed Satellite Service (CFSS) provides satellite capacity that can be used to deliver communications and applications at a customer-specified throughput between two or more specified end points. This service can be used for applications such as distance learning, continuity of operations, broadcast video and associated audio, including encrypted communications.

C.2.7.1.2 Standards

This section addresses CFSS standards. The air interface for a government-owned or -controlled earth terminal shall be at the terminal antenna. Government-owned terminals will provide the capability of handling multiple CFSS carriers. The government terminals shall be considered as conforming to the mandatory requirements of Military Standard (MIL-STD)-188-164 with associated modems conforming to MIL-STD-188-165.

Satellite services are required to be provisioned by the contractor in accordance with the following priority:

1. Utilization of satellites compliant with DODI 8581.01.
2. Utilization of other available satellites when DODI 8581.01 compliant satellites are not available shall be contingent upon the cognizant CO and COR accepting the associated risk.

For CMSS, the contractor shall support the following standards:

1. North American Numbering Plan (NANP)
2. ITU-TSS World Numbering Plan (Standard: ITU-TSS E-164)
3. IETF RFCs for IPv4/v6
4. Proprietary air-link interface standards based on mobile satellite systems, such as the Inmarsat Broadband Global Area Network (BGAN) and the Iridium satellite constellation

The contractor shall provide domestic and non-domestic satellite services when required in the TO.

C.2.7.1.3 Technical Capability

The contractor shall provide space segments to meet the requirements specified in the TO and, at a minimum, the performance requirements specified in Section C.2.7.3. For dedicated capacity requirements, the contractor shall provide satellite bandwidth on a non-preemptable basis unless otherwise specified in the TO. That is, the bandwidth shall not be preempted for any reason, and shall be replaced in the event of failure.

The contractor shall provide contractor-operated and -maintained leased earth terminal services as specified in individual TOs. Earth terminals provided by the contractor shall be certified as acceptable for service by the satellite system operator of the specific system on which the earth terminal is to be used.

The contractor shall provide CFSS Satellite Internet Service (SIS). The SIS shall provide Internet access as well as domestic and international voice service.

For CMSS, the contractor shall support Internet access, voice calling, SMS texting, fax, streaming services, and M2M.

C.2.7.2 Features

The following CFSS features are mandatory for delivery of COMSATCOM:

1. Capacity: The contractor shall be able to provide scalable capacity in any available COMSATCOM frequency band in support of US Government COMSATCOM requirements, subject to the availability of satellite resources.
2. Coverage: The contractor shall be able to provide coverage anywhere worldwide in any available COMSATCOM frequency band, including, but not limited to, L-, S-, C-, X-, Ku-, extended Ku-, Ka-, and UHF. Specific pre-defined coverage may be negotiated and defined in the TO. This requirement is subject to the availability of satellite resources.
3. Network Monitoring (Net OPS): The contractor shall have the capability to electronically collect and deliver near real-time monitoring, fault/incident/outage reporting, and information access to ensure effective and efficient operations, performance, and availability, consistent with commercial practices. The Net OPS information will be provided on a frequency (example: every 6 hours, daily) and format (example: SNMP, XML) consistent with the contractor's standard management practices, to a location/entity/electronic interface as defined in a requirement by the OCO. Specific reporting requirements will be defined by the OCO.
4. EMI/RFI Identification, Characterization, and Geo-location: The contractor shall have the capability to collect and electronically report in near real-time Electro-Magnetic Interference (EMI) / Radio Frequency Interference (RFI) identification, characterization, and geo-location, including the ability to identify and characterize sub-carrier EMI/RFI being transmitted underneath an authorized carrier, and the ability to geo-locate the source of any and all EMI/RFI. The contractor shall establish and use with the OCO a mutually agreed-upon media and voice communications capability capable of protecting CUI data.

5. Interoperability (Net Ready): COMSATCOM services shall be consistent with commercial standards and practices. Services shall have the capability to access and/or interoperate with government or other commercial teleports/gateways and provide enterprise service access to or among networks or enclaves.
6. Information Assurance: The contractor shall meet the following standards as applicable:
   a) The Committee on National Security Systems Policy (CNSSP) 12, "National Information Assurance Policy for Space Systems used to Support National Security Missions," or
   b) DODI 8581.1, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense."

The contractor shall demonstrate the ability to comply with FISMA as implemented by Federal Information Processing Standards Publication 200 (FIPS 200), "Minimum Security Requirements for Federal Information and Information Systems." At a minimum, all services shall meet the requirements assigned against a low-impact information system (per FIPS 200) that is described in the current revision of NIST SP 800-53, "Security Controls for Federal Information Systems and Organizations."

The contractor's information assurance boundary is defined as where the contractor's services connect to the user terminals/equipment (i.e., includes satellite command encryption (ground and space); systems used in the Satellite Operations Centers (SOCs), Network Operations Centers (NOCs) and teleport; and terrestrial infrastructure required for service delivery).

For CMSS, the contractor shall provide satellite phones/terminals (dual-mode (satellite/GSM) and tri-mode (satellite/CDMA/AMPS)) and encrypted transmission.

C.2.7.3 Performance Metrics

The contractor shall provide domestic and non-domestic CFSS and CMSS as specified in the table below.

Satellite Performance Requirement (KPI)	Performance Specification (Threshold/AQL)
Availability (for both CFSS and CMSS)	≥ 99.5%
For CFSS:	
Error Free Seconds (EFS)	> 0.965
Severely Errored Seconds (SES)	≤ 0.0003
Degraded Minutes (DM)	≤ 0.02

Mean Time to Loss of BCI (MTTLBCI)	≥ 24 hours
Delay (One Way)	The lesser of 450 ms or (260 + 0.01 x D ms) (See Note 2)

Notes:

1. CFSS and CMSS availability is calculated as a percentage of the total reporting interval time that they are operationally available to the agency. Availability is computed by the standard formula:

$$Av(CFSS\ \&\ CMSS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. "D" is the SDP-to-SDP transmission distance, measured via the shortest great circle, in kilometers.

C.2.8 Managed Service

Managed service is the practice of outsourcing day-to-day customer management responsibilities and functions to the service provider as a strategic method for improving operations and cutting expenses. The managed service provider is accountable for the functionality and performance of the managed service.

Managed services provide the delivery and management of network-based services, applications, solutions, labor and equipment needed to the enterprises. The managed service includes a) service planning and solution engineering, b) solution implementation (including labor and equipment), c) service provisioning, d) end-to-end service management (including LAN routers and WAN), and e) service assurance (performance metrics and SLA management).

C.2.8.1 Managed Network Service

C.2.8.1.1 Service Description

Managed Network Service (MNS) enables an agency to obtain design and engineering, implementation, management, and maintenance services for agency networks. MNS provides the necessary technical and operational capabilities that ensure the availability and reliability of agencies' increasingly complex networks.

When MNS is used with a single EIS service (e.g., VPNS) or a group of EIS services (e.g., VPNS, Ethernet, voice service, and cloud IaaS) requested in a TO, those services will have the functionalities of a managed service (i.e., Managed VPNS, Managed Ethernet, Managed voice service, and Managed Cloud IaaS).

The contractor shall use the appropriate labor and equipment as defined in Section C.2.10 Service Related Equipment and Section C.2.11 Service Related Labor in the TO.

C.2.8.1.1.1 Functional Definition

Under the MNS offering, the contractor provides overall management of an agency's network infrastructure, including real-time proactive network monitoring, troubleshooting and service restoration. The contractor is the agency's single point of accountability for all networks managed under this service, including operations, maintenance, and administration activities.

C.2.8.1.1.2 Standards

MNS shall comply with the following standards:

1. All appropriate standards for any underlying EIS access and transport services
2. The specific standards and requirements identified in the TO

C.2.8.1.1.3 Connectivity

MNS shall work with underlying EIS offerings such as VPNS, PLS and other services as needed, to ensure seamless connectivity to agency networking environments.

C.2.8.1.1.4 Technical Capabilities

The following MNS capabilities shall be provided by the contractor.

C.2.8.1.1.4.1 Design and Engineering Services

The contractor shall provide design and engineering services that include, but are not limited to:

1. Identify hardware and firmware (e.g., routers, switches, and other SRE), related software, and SRL required by the agency to deliver the EIS services.
2. Identify network components and determine protocols, redundancy, traffic filtering, and traffic prioritization requirements. Recommend the appropriate performance levels and network capacities as required.
3. Provide complete project management for design, engineering, implementation, installation, access coordination, provisioning, equipment configuration, hardware testing, and service activation. Coordinate installation activities with the agency to minimize the impact on the current networking environment.

C.2.8.1.1.4.2 Implementation, Management and Maintenance

1. The contractor shall develop, implement, and manage comprehensive solutions using the EIS services to meet agency-specific requirements. The solutions shall include, but are not limited to:
   a) Access solutions that use a combination of different services (e.g., wireline and wireless access services) for specific agency locations, to meet agency performance metrics for availability and disaster recovery.
   b) Transport solutions that distribute traffic over multiple contractor backbone networks to provide redundancy and carrier diversity, and vary the traffic allocation dynamically based on agency performance requirements.
   c) Customer premises solutions that provide agency-specific interfaces, software, and equipment to meet agency requirements.
   d) Security solutions as required by the agency.
2. The contractor shall supply and manage the hardware, firmware and related software required by the agency. Components include but are not limited to routers and switches, encryption devices, CSUs/DSUs, hubs, adapters, and modems.
3. The contractor shall provide tools to:
   a) Monitor performance of agency-specific networks including transport services, access circuits, and government edge routers
   b) Provide real-time visibility of transport and access services performance
4. The contractor shall:
   a) Manage the network in real-time on a 24x7 basis
   b) Support remote management capabilities from the operations center defined in the TO
   c) Proactively monitor utilization and performance, probing in intervals of no more than fifteen minutes to ensure proper equipment/network operations
   d) Assess and report access and transport services performance and SLAs
   e) Assess and report on agency-specific network capacity and performance
   f) Address agency-specific network capacity and performance issues
5. The contractor shall permit SNMP read-access data feeds that provide the agency with managed equipment information, as applicable.
6. The contractor shall manage network configuration. Activities shall include but are not limited to the following:
   a) Adding a protocol
   b) Adding, moving or removing Customer Premises Equipment (CPE)
   c) Changing addressing, filtering, and traffic prioritization schemes

d) Optimizing network routes
e) Updating equipment software and/or configuration, including but not limited to firewall and VPN security devices
f) Upgrading or downgrading bandwidth
g) Implementing configuration changes for all agency-specific devices
h) Maintaining a configuration database for all agency-specific devices
i) Auditing government router configurations

7. The contractor shall provide IP Address Management as applicable. The contractor shall submit agency-completed American Registry for Internet Numbers (ARIN) justification requests for specified IP allocations in order to support the service offered.
8. The contractor shall monitor and control access to equipment under its control including limiting access to authorized personnel, and implementing passwords and user permissions as directed and approved by the agency.
9. The contractor shall regularly perform off-site equipment configuration backups, in order to ensure the availability of recent configuration data for restoration purposes. The contractor shall provide the agency with secure access to backup logs as needed.
10. The contractor shall perform necessary hardware and software upgrades, updates, patch deployments and bug fixes as soon as they become available. The contractor shall implement updates in coordination and mutual agreement with the agency and test new releases to resolve any security concerns, ensure compatibility with the agency environment, minimize service disruptions, and maintain equipment functionality.
11. The contractor shall provide preventative and corrective maintenance on agency-specific devices.
12. The contractor shall proactively detect problems, respond to alerts and promptly report situations that adversely affect throughput to the agency. The contractor shall provide notification of alarms, network troubles and service interruptions via email, telephone, or as specified in the TO. The contractor shall:
    a) Monitor agency-specific network availability and quality of service (e.g., network delays, packet loss)
    b) Monitor access circuit availability and QoS
    c) Monitor the government's edge router availability and performance
    d) Monitor transport service availability at the government's network equipment

e) Monitor agency-specific network performance from government network equipment to government network equipment
f) Monitor transport service availability up to the government's network equipment
g) Monitor transport service performance from government network equipment to government network equipment
h) Provide, monitor and manage circuits for out-of-band government network equipment management
i) Open/close trouble ticket in agency's trouble ticketing system
j) Open/close trouble ticket in contractor's trouble ticketing system
k) Troubleshoot access and transport services faults and coordinate faults resolution/repairs
l) Troubleshoot government network equipment faults and coordinate resolution/repairs.
m) Troubleshoot agency-specific network faults
n) Notify agency-specific network users of faults and maintenance via agency alerts
o) Answer NOC Help Desk phones and provide Tier-1 support to agency-specific network users
p) Provide Tier-1/Tier-2/Tier-3 support to agency NOC for contractor access and transport services
q) Provide Tier-1/Tier-2/Tier-3 support to agency NOC for the components of the Agency's network that are managed by the contrtactor.

13. The contractor shall provide the agency with real or near-time access to the following:
    a) Installation schedule detailing the progress of activities such as the implementation of equipment, access and transport circuits, and ports, as applicable. This allows agencies to track the provisioning process through completion at any time. Near real-time access to the installation schedule is acceptable.
    b) Network statistics and performance information including equipment data availability, throughput and delay statistics, CoS settings, and application-level performance information.
    c) Trouble reporting and ticket tracking tools
    d) Security logs
14. The contractor shall provide inventory tracking tool(s) to maintain and track all agency circuit, transport service and equipment inventory information.
15. The contractor shall provide the agency with secure access to current and historical information which includes, but is not limited to, the following:

a) Bandwidth and service quality information
b) Burst analysis identifying under or over utilization instances
c) Data errors
d) Delay, reliability and data delivery summaries
e) End-to-end network views
f) Exception analysis
g) Link, port and device utilization
h) Network statistics
i) Protocol usage
j) CPU utilization
k) Traffic, port and protocol views

C.2.8.1.2 Features

The contractor shall provide the following features:

1. GFP and SRE Maintenance. The contractor shall maintain and repair GFP and SRE.
2. Agency-Specific Network Operations Center (NOC) and Security Operations Center (SOC). The contractor shall provide agency-specific help desk services and shared or dedicated NOCs and SOCs to meet agency requirements.
3. Network Testing. The contractor shall support agency-specific development services which address the agency‘s potential need to test equipment, software and applications on the contractor’s network prior to purchase and deployment. This shall cover voice, data, and video technologies that include but are not limited to IP VPN and voice services. Testing shall be performed at the agency’s discretion and structured in collaboration with the contractor.
4. Traffic Aggregation Service (DHS Only). The contractor shall establish and maintain secure facilities ("DHS EINSTEIN Enclaves") where DHS-furnished equipment can be deployed, provide network connectivity from the DHS EINSTEIN Enclave to the DHS data centers, and route all traffic subject to National Policy requirements described in Section C.1.8.8 through (i.e., deliver to and receive from) a DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN capabilities. Once traffic is received at the EINSTEIN Enclave and processed, it is sent back to the contractor for delivery to its destination. The contractor shall assume responsibility for maintaining and repairing the traffic aggregation service, including associated commercial security services and all communications links, and shall provide engineering support to

integrate the DHS GFP sensor equipment, data center and communications infrastructure into the contractor's services. The contractor shall assist DHS in the maintenance and repair of the sensor system to the extent of receiving phone calls or emails requesting "Smart-Hands" service of DHS-supplied equipment.

C.2.8.1.3 Interfaces

MNS shall support the UNIs for all underlying EIS access and transport services.

C.2.8.1.4 Performance Metrics

The MNS performance levels will be specified in the TO.

C.2.8.2 Web Conferencing Service

C.2.8.2.1 Service Description

Web Conferencing Service (WCS) enhances traditional conferencing by offering the capability to meet, present, and interact with information via a web browser.

C.2.8.2.1.1 Functional Definition

WCS allows agencies to share information, documents, or applications interactively via the Internet and the agency's Intranet.

C.2.8.2.1.2 Standards

WCS shall comply with the following standards:

1. Hyper Text Transfer Protocol (HTTP)
2. Hyper Text Transfer Protocol Secure (HTTPS)
3. (Optional) IETF RFC 3261 for Session Initiation Protocol (SIP)
4. ITU-T T.120 Series of Data Protocols for Multimedia conferencing
5. Transport Layer Security (TLS) Encryption
6. Transmission Control Protocol/Internet Protocol (TCP/IP) Suite

The contractor shall comply with new versions, amendments, and modifications made to the standards listed above.

C.2.8.2.1.3 Connectivity

WCS shall connect to and interoperate with:

1. Agency Intranet
2. Internet

WCS shall be accessible via a Universal Resource Locator (URL) address.

C.2.8.2.1.4 Technical Capabilities

The following WCS capabilities are mandatory unless marked optional:

1. The contractor shall provide a capability that enables participants to collaborate. This shall include real-time document sharing, file transfer capability and electronic whiteboards in a private and secure WCS session.
2. The contractor shall provide the following capabilities:
   a) Authentication and password protection
   b) Customized greeting (or message) screen
   c) Online Help
   d) Support for point-to-point and multi-point Web conferences
3. The WCS shall interoperate with the Internet and ordering agencies' IP network(s).
4. The WCS shall be compatible with available Web browser software packages. Appropriate plug-ins shall be provided in order to deliver WCS to the user.
5. The contractor shall provide a means by which users can test and verify that their web browser and desktop software are compatible with WCS service prior to the scheduled conference. If required, the contractor shall provide the appropriate plug-ins to deliver WCS to the users. The browser plug-in shall be limited to utilities required for the user to play back, participate in, or lead a web conference session. This can include plug-ins that enable users to play back recorded conferences from their web browser, develop WCS presentation slides within existing agency-owned software applications (i.e. Microsoft PowerPoint) or view WCS from mobile devices.
6. The WCS shall support dynamic content (i.e., the ability to use Audio Visual Interleave (AVI's) files, flash, animated gif, and dynamic html pages).
7. The WCS shall be available on demand or via a scheduled reservation.
8. The contractor shall provide a reservation system with the ability for authorized WCS users to schedule or cancel web conferences at least one year in advance. Scheduling may be by time and day of the week, either as a single event or recurring event on a daily, weekly, monthly, or on another periodic basis.
9. The contractor shall provide an email notification with a meeting invitation and RSVP to WCS participants.
10. The contractor shall provide the capability to extend the scheduled conference time upon request from the ordering agency and to add participants.
11. The WCS shall be secure and provide authentication and encryption capabilities to identify and authenticate users before providing access.
12. The WCS shall be accessible via a Universal Resource Locator (URL) address with a login and password for valid participants.

13. The contractor shall provide passwords for both conference leaders and participants.
14. The WCS shall provide the capacity to support at least 1,000 simultaneous participants in an individual Web conference.
15. The WCS shall have the capability to traverse and successfully interoperate with agency firewalls and security layers. The contractor shall verify with the agency that the agency firewall is compatible with this service.
16. The contractor shall provide the capability for users to request operator assistance to immediately resolve WCS service issues or problems.
17. The WCS shall provide annotation (i.e., the ability to emphasize a specific area of a presentation slide with a marker or pointer tool).
18. The WCS shall provide a participant list (i.e., the ability to view the names of other participants attending the WCS presentation).
19. The contractor shall support group web surfing (i.e., the ability for the conference leader to guide and navigate WCS participants to a web page).
20. The contractor shall support file transfer (i.e., the ability to upload a file that a WCS participant can download within the meeting or event). The file transfer can be sent to all participants or selected participants. The receiving participant shall have the option to accept or reject the file transfer.
21. The contractor shall support multiple presenters on a WCS meeting or event.
22. The contractor shall support video webcasts to no fewer than 3,500 participants.
23. The contractor shall provide polling and voting capability. This allows the conference leader to pose questions and receive feedback from participants during a presentation with a variety of different answer sets (multiple choices, open ended, yes/no) on demand. The participant shall have the capability to signal the conference leader when they have a question.
24. WCS polling/voting feedback shall be available instantly for the WCS conference leader and, if requested, via a polling/voting results report.
25. (Optional) The contractor shall provide a meeting lobby to allow conference leaders to admit participants to the meeting, as well as the ability for conference leaders to lock and unlock access to the meeting. When the meeting is “locked,” no additional participants are allowed to join the active conference.
26. The contractor shall provide the capability for conference leaders to print the presentation used during the conference or save it to a local file. Participants shall have the same capability if permitted by the conference leader.
27. WCS shall support text chat, which enables real-time text communications between WCS conference participants. This shall include support for a public text chat for all participants with the conference leader, and private chats between selected participants.

28. The contractor shall provide the capability to present a survey to all or a random percentage of participants to gather feedback and/or capture customer satisfaction data.

C.2.8.2.2 Features

The following WCS features are mandatory unless marked optional:

1. Streaming Audio: The contractor shall provide the ability to deliver one-way audio over the Internet during a WCS session. The streaming audio shall be synchronized with any data portions of the Web conference.
2. Streaming Video: The contractor shall provide the ability to deliver one-way video over the Internet during a WCS session. The streaming video shall be synchronized with any data portions of the Web conference.
3. Web Based Presentation Replay: The contractor shall provide the capability to replay (or play back) Web-based presentations. The replay shall be available for a minimum of 90 days after the initial conference. The contractor shall offer the agency an option for extending the conference replay, in 30-day increments, for a period of 1 year.

C.2.8.2.3 Interfaces

Not applicable – WCS is a browser based service.

C.2.8.2.4 Performance Metrics

The performance levels and AQL of KPIs for WCS in Section C.2.8.2.4.1 are mandatory unless marked optional.

C.2.8.2.4.1 Web Conferencing Service Performance Metrics

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability	Routine	99.9%	≥ 99.9%	See Note 1
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Availability is measured and calculated as a percentage of the total reporting interval time that WCS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

.

C.2.8.3 Unified Communications Service

C.2.8.3.1 Service Description

Unified Communications Service (UCS) integrates multiple methods of communication, (e.g., e-mail, faxing, instant messaging, voice and video calling, conferencing that identifies which participant is speaking, mobile communication, and desktop sharing) in order to allow users to connect, collaborate, and exchange information. This may include real-time and non-real-time, “one-to-one”, “one-to-many”, and “many-to-many” bi-directional communications between internal and external entities. UCS can be implemented as an application hosted by the contractor that supports multiple users over an IP network (agency- or contractor-provided), or as a premises-based, hosted, or hybrid solution.

UCS combines independently-run communications subsystems in order to streamline how agency users and customers communicate and collaborate regardless of location.

C.2.8.3.1.1 Functional Definition

UCS supports a common user interface for agency communications subsystems, such as voice subsystems (VoIP based/enabled) and applications, including unified messaging, instant messaging, presence, voice mail, integration with email where applicable, fax, and video/ audio/web conferencing, and allows users to access messages with any device, anywhere, and at any time.

C.2.8.3.1.2 Standards

UCS shall comply with the following standards:

1. All applicable IETF RFCs for IP-based voice, data, and video applications, such as VoIP (SIP), TCP/IP, mail (SMTP, POP3, IMAP4, LDAP), and RSVP for call admission.
2. Common telephony and network standards, including but not limited to:
   a) SIP/SDP for call setup and trunking
   b) SRTP and G.711/G.722/G.729/H.264/OPUS CODEC, IETF RFC 6716 CODEC
   c) DSCP and LLDP for network traffic prioritization and device provisioning
   d) TLS and MTLS for session security
   e) ICE/STUN/TURN for NAT traversal and media relay for clients outside the firewall

f) XMPP/SIP/PIDF for IM/presence federation

3. The specific standards as identified in the TO.
4. All appropriate standards for any applicable underlying EIS access and transport services.

C.2.8.3.1.3 Connectivity

UCS shall connect to and interoperate with:

1. PSTN (SIP trunk gateway).
2. Agency communication subsystems (e.g., voice, email, conferencing (audio, web-based video), instant messaging, presence, collaboration portals), over an IP network (agency provided or contractor provided).

C.2.8.3.1.4 Technical Capabilities

The following UCS capabilities are mandatory unless marked optional:

1. The contractor shall support enabling UC capabilities via many devices, including desktop phones and mobile devices (smart phones, tablets, etc.), wireline and IP phones, soft clients, and video conferencing devices.
2. Unified Messaging (UM) shall provide:
   a) User access to and management of voice mail, e-mail and fax messages through the same inbox or interface.
   b) Modular messaging with access to messages from phones and PCs via various interfaces, including browsers.
   c) The UC Messaging Directory, which acts as a container for all the UM objects and their configuration settings, shall logically represent a telephony hardware device and a telephony dial plan for the enterprise to support a specific UM feature.
   d) The UC Messaging Directory objects shall enable the integration of UM with existing telephony infrastructure. The following UM objects shall be supported:
      i. Dial Plans
      ii. Mailbox Policies
      iii. IP Gateways
      iv. Hunt Groups
      v. Auto Attendants
      vi. Servers
      vii. Users
3. Mobile Integration shall:

a) Provide users with a single identity that lets them handle business calls via their desk and mobile phones.
b) Provide users the ability to have calls forwarded to any phone and to use a single number for making and receiving all calls.
c) Support handing off calls from cellular to Wi-Fi connections and vice versa on smart phones.
d) Enable users to initiate phone calls, retrieve voice mail and corporate directories, access instant messaging and participate in video conferencing.
e) Provide features that are accessible from mobile phones, laptops and tablets, provide access to corporate directories and visual voice mail, and feature seamless handoff between cellular and Wi-Fi calls.
f) Allow calls to or from mobile devices to take place anywhere and anytime as if they are going to / coming from the desk phone numbers.

4. The Unified User Interface shall provide:
   a) The ability for users to access UC capabilities from a variety of devices in a variety of ways.
   b) Features such as presence, instant messaging, integrated soft phones, voice conferencing, video calling and conferencing.
   c) Voice activation that integrates seamlessly with other business communication systems.
   d) Real-time communications – instant messaging, presence that identifies which participant is speaking, voice calls to video, voice calls to email.
   e) Non-real time communications – email, text messaging, fax, voice mail.
   f) Collaboration and data sharing – electronic bulletin boards, e-Calendar, Audio/Video/Web conferencing.
   g) The ability for users to access messages from the following:
      i. IP phones
      ii. Mobile phones
      iii. (Optional) Web browsers
      iv. E-mail clients
      v. Desktop clients
      vi. PCs
      vii. Tablets
   h) Instant messaging between two users or multiparty (up to an agency-defined number of participants).

i) The ability for users to display their presence status (e.g., “Available,” “Away,” “Do Not Disturb,” “Busy,” or Offline) to let others know their availability for communication.

j) Presence integration with agency collaboration applications, such as calendaring, that automatically updates presence when users are in a meeting.

k) Audio and video conversations between two users or multiparty (up to an agency-defined number of participants), using web cameras, speakers and microphones.

l) File Transfer capabilities to send files between users.

m) Scheduled and ad hoc web conferencing for conducting online presentations including audio, video, screen sharing, and a virtual whiteboard. PC-to-PC and multiparty data sharing capabilities including desktop sharing, application sharing, presentations, virtual whiteboard, annotations, and polling.

n) Contact Groups that allow users to organize their contacts.

o) (Optional) Enhanced access to instant messaging from within the agency's enterprise network or from the Internet, through a variety of devices and software, in a secured mode using encryption.

p) Agency-managed instant messaging administration (add/change/delete users).

q) Single sign-in capabilities through the agency’s Enterprise Active Directory (EAD) system.

r) Automated and/or staffed UCS-dedicated Service Desk available 24/7.

5. The contractor shall provide the following capabilities to support QoS, if UCS is provided over the contractor’s IP network:
   a) Configuration Options for QoS
   b) Traffic Prioritization
   c) QoS Queuing Methods and Scheduling
6. (Optional) The UCS shall provide a premises-based WAN optimizer to collect only the changes from each site, if the compilation of the current status of all users being logged on is transmitted over the agency WAN.
7. The UCS shall support both IPv4 and IPv6 and be able to communicate over IPv4-only, IPv6-only, and/or dual-stack networks.
8. The UCS shall meet a minimum voice quality level that is equivalent to or better than a Mean Opinion Score (MOS) of 4.0 as specified in ITU-T specification P.800 series.

9. The contractor shall ensure that security practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized access. This includes SIP-specific gateway security for SIP firewalls where applicable. The contractor shall also comply with agency-specific security policies, regulations and procedures.

C.2.8.3.2 Features

None.

C.2.8.3.3 Interfaces

The contractor shall support UCS to different devices. At a minimum, the following shall be supported:

1. IP phones
2. Mobile phones
3. Web browsers
4. E-mail clients
5. Desktop clients
6. PCs
7. Tablets

C.2.8.3.4 Performance Metrics

The UCS performance levels and AQL of KPIs in Section C.2.8.3.4.1 are mandatory unless marked optional.

C.2.8.3.4.1 UCS Performance Metrics

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Note:

1. Availability is measured and calculated as a percentage of the total reporting interval time that UCS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

C.2.8.4 Managed Trusted Internet Protocol Service

C.2.8.4.1 Service Description

The requirements for government department and agency cybersecurity are evolving to incorporate advanced methods of aggregating and segregating inbound and outbound Internet traffic, Intrusion Detection, Intrusion Prevention, anti-virus and other services as supported by evolving commercially provided cyber-protection capabilities. Existing requirements are stated in this Section and will be updated according to DHS reference standards and OMB instructions in place at the time the RFP is issued.

The Managed Trusted Internet Protocol Service (MTIPS) allows agencies to physically and logically connect to the public Internet or other external connections, as required by the agency, in full compliance with the Office of Management and Budget's (OMB) Trusted Internet Connections (TIC) initiative (M-08-05), announced in November 2007 and subsequent modification to TIC 2.0, issued by the Department of Homeland Security (DHS). MTIPS facilitates the reduction of the number of Internet connections in government networks and provides standard security services to all government users.

MTIPS solutions offered by the contractors have been and shall be subject to periodic DHS Cybersecurity Compliance Validation (CCV) formerly known as TIC Compliance Validation (TCV). The Department of Homeland Security (DHS) is responsible for the "Compliance and Assurance Program (CAP)". The CAP employs a collaborative approach and measures, monitors and validates the implementation of cross-government initiatives and assesses cyber risks. Under CAP, MTIPS subscriber agencies shall complete an annual Cybersecurity Compliance Validation (CCV) self-assessment and DHS will conduct an on-site CCV every three years. The MTIPS contractors shall participate in an annual DHS led CCV assessment.

MTIPS is comprised of the network infrastructure to transport IP traffic between the agency Enterprise WAN and the TIC Portal; together they create an agency TIC Trusted Domain (DMZ) for IP traffic. In today's environment, the agency perimeter boundary is dynamic and morphing to include virtual instances.

MTIPS enables the government to react more effectively to cyber security attacks thus reducing malicious penetrations and theft of critical data. Exchange of information

through the TIC Portal is closely monitored by an integral MTIPS Security Operations Center (SOC) to protect agency IP traffic.

The MTIPS provided transport shall serve as a “collection” network for TIC physical or virtual Portal connectivity insulating an agency’s internal network from the Internet and other external networks.

The TIC Portal shall function as an OMB approved Multi-Service Trusted Internet Connection Access Provider (TICAP) capable of hosting multiple agencies and able to manage and correlate multiple independent traffic streams for each ordering agency. The TIC Portal shall provide physical and virtual security services to multiple government clients, but allow for specific controls based on agency coordination, when necessary.

Each contractor shall build at a minimum two (2) TIC Domestic Portals that maintain physical diversity from the TIC Portals to its servicing Internet Exchange Point. The contractor shall provide management staff at each TIC Portal.

The contractor shall provide virtual TIC capabilities upon request for agencies with resources hosted outside their physical boundaries.

C.2.8.4.1.1 Functional Definition

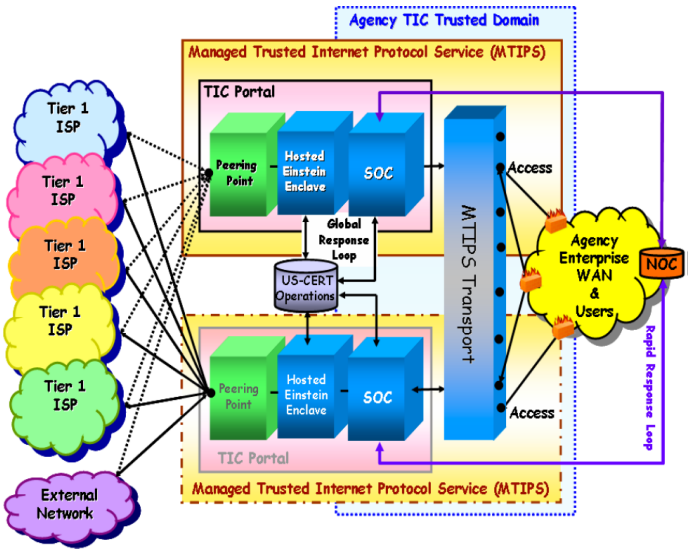
The MTIPS generic functional model consists of the following set of functions and sub functions:

1. TIC Portal (TIC Access Points):
    a) Access to External Networks including the Internet
    b) Routing of traffic through EINSTEIN Enclave
    c) Security Operations Center (SOC)
2. Transport Collection and Distribution (MTIPS Transport)

The traffic collection and distribution supports the transport of government-only IP traffic between agency Enterprise network and TIC Portals utilizing the secure functionality of the SOC. The TIC Portal SOC monitoring and management systems shall be dedicated to the management and monitoring of the ordering agencies hosted by the contractor’s portal and shall be isolated from commercial customers.

The MTIPS Context Architecture is defined in Figure C.2.8.4.1.1.1 below. The TIC Portal Security Operations Center Architecture is defined in Figure C.2.8.4.1.1.2.

C.2.8.4.1.1.1 MTIPS Context Architecture



C.2.8.4.1.1.2 TIC Portal Security Operations Center Architecture

C.2.8.4.1.2 Standards

MTIPS shall comply with the following standards:

1. Current and future regulations, policies, requirements, standards, and guidelines for Federal U.S. Government technology and cyber security (e.g., the TIC Reference Architecture document) and within 90 days develop a plan for adoption. The contractor shall submit the plan to the CO within 90 days of issuance of new TIC capabilities or policy changes.
2. New document versions, amendments, and modifications. The most notable include minimum expectations for identified MTIPS-specified security services.

C.2.8.4.1.3 Connectivity

The MTIPS contractor shall connect and interoperate with:

1. The Public Internet
2. EINSTEIN Enclave
3. Global Response Loop to US-CERT with a cross-agency view that allows for coordination across TIC Portals

4. Rapid Response Loop from DHS to agency communications for the dissemination of threats/events to/from the agency
5. Other Agency IP Networks (External or Internal Connections)

C.2.8.4.1.4 Technical Capabilities

C.2.8.4.1.4.1 TIC Portal Capabilities

The following TIC Portal capabilities are mandatory, unless marked optional:

1. TIC Portal Access to External Networks including the Internet – To ensure that agencies are able to exchange traffic with the Internet and external networks at all times the TIC Portal shall comply with the following requirements when establishing interconnecting relationships:
   a) The TIC Portals shall connect to the Internet via Tier 1 Internet Service Providers (ISPs).
   b) The contractor shall budget enough interconnection bandwidth to accommodate increasing agency's demands.
   c) Alternate and diverse Routing – The contractor's TIC Portal shall provide multiple, physically diverse connectivity to interconnection points. The contractor shall consider single and multiple failure scenarios in the development of the technical architecture to demonstrate that KPIs and SLAs required in this document are met.
   d) Inter-carrier Routing Requirements – The ISPs and external networks converging to a portal shall run BGP (eBGP, BGP4, etc.) or one of the options for inter-AS connectivity as specified by the IETF.
   e) Support to Internet Protocol version 6 (IPv6) – The contractor shall also transport both IPv4 and IPv6 (i.e. dual-stack) between external connections, including the Internet, and agency's internal networks.
2. EINSTEIN Protection – The EINSTEIN Enclave includes the EINSTEIN devices providing customized threat mitigation, analytic, and network flow capabilities. The enclave in its entirety is provided by the government through separate means. At each TIC Portal the contractor shall meet applicable routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.
3. TIC Portal Security Operations Center (SOC) – The TIC Portal SOC is the set of tools, appliances and processes that collect, reduce, normalize, correlate, fuse, and manage event data from a variety of devices that support the MTIPS operations. For the SOC, these devices include firewalls, Network Intrusion Detection Devices (NIDS), Host-based IDS (HIDS), and other platforms that may collect TIC Portal-relevant event data. The SOC tools also provide reports customized to agency's requirements but as a minimum shall support TIC Portal

authorities / analysts by identifying security events of interest that may be negatively affecting the TIC Portal environment. The ordering agency's security authorities / analysts then will be empowered to react and trigger appropriate control mechanisms, thus creating a Rapid Response Loop. The primary goal of the SOC is to provide analysis/correlation and management structure to mitigate the threat presented by external attacks. Provide trained, qualified, and cleared staff (U.S. citizens) to support security functions 24x7. The SOC shall be staffed with at least two (2) people with appropriate credentials to manage technical aspects of the network attacks. The contractor shall comply with DHS-published TIC 2.0.

4. Reserved. .
5. Content Filtering/Inspection of Encrypted Traffic with documented procedures.
6. Asymmetric Routing – The MTIPS portal stateful inspection devices shall correctly process traffic returning through asymmetric routes to a different MTIPS stateful inspection device; or shall document how return traffic is always forced to return to the originating MTIPS portal stateful inspection device.
7. Federal Video Relay Service (FedVRS) Support – The MTIPS portal shall support Federal Video Relay Service (FedVRS) for the Deaf (www.gsa.gov/fedrelay) network connections, including but not limited to devices implementing stateful packet filters.
8. E-Mail Forgery Protection – Domain-level sender forgery analysis equivalent to Domain Keys Identified Mail or Sender Policy Framework standards.
9. The contractor shall optionally support signing procedures for outgoing email messages to ensure that they have been digitally signed at the Domain Level (for example Domain Keys Identified Mail).
10. Domain Name System (DNS) and DNS Security Extensions (DNSSEC) – The MTIPS portals shall be equipped with resolving/recursive (also known as caching) name servers to properly filter DNS queries, and to perform validation of DNS Security Extensions (DNSSEC) signed domains for MTIPS subscribers. (Reference: NIST SP 800-81 Revision 1)
11. Uninterrupted Operations – The MTIPS portals shall be equipped for uninterrupted operations for at least 24 hours in the event of a power outage
12. Internet Protocol Version 6 (IPv6) – The contractor shall ensure that all TIC systems and components of the TIC portals support both IPv4 and IPv6 protocols in accordance with OMB Memorandum M-05-22, and the "IPv6 Transition Guidance" issued by the Federal CIO Council, Architecture and Infrastructure Committee."
13. Data Loss/Leak Prevention – The contractor shall support Data Loss (Leak) Prevention (DLP) program.

C.2.8.4.1.4.2 MTIPS Transport Collection and Distribution Capabilities

The following MTIPS Transport Collection and Distribution Capabilities are mandatory unless marked optional:

1. The contractor shall allow the agency's Internet bound traffic to reach the Internet via one of the two TIC Portals.
2. An agency Trusted Domain (DMZ) shall be created by the contractor to ensure that an agency's traffic is protected and physically isolated when transported to the portal and the public Internet. The DMZ includes the access portion of the service as well as the MTIPS transport. The contractor shall ensure that the traffic is not sniffable and ports cannot be spoofed.
3. Inter-agency traffic shall be routed through and inspected by the TIC Portal if the connection is classified as an external connection.

C.2.8.4.2 Features

1. Encrypted Traffic: The TIC Portal shall monitor, scan and filter the incoming and outgoing encrypted traffic traversing MTIPS (e.g., email, authorized / known bad mail, FTP and web traffic) which is proxied / non-proxied based on URL or IP address. The TIC portal shall analyze all encrypted traffic for suspicious patterns that might indicate malicious activity and shall keep logs of at least the source, destination and size of the encrypted connections for further analysis.
2. Agency Security Policy Enforcement: The contractor shall adhere to and support the ordering agency's security policy to ensure security regulations compliance. The contractor shall support agency's operational models and specific security rules. These shall be negotiated between the agency and the contractor. The contractor shall support adjustments to the agency's security strategy based on threats identified by the TIC Portal SOC. For example, adjustments to the security policy could be made by the agency's authorities after the SOC identifies changing trends in intrusion behavior.
3. Forensic Analysis: The contractor shall support full, real-time, header and payload, raw packet capture of selected agency's traffic flows and shall support subsequent forensic traffic analysis of cyber incidents as required by the agency (administrative, legal, audit or other operational purposes). The agency will identify technical requirements such as, but not limited to traffic of interest (relevant traffic to capture). The agency will require support to engineering parameters applied to the traffic capture such as, but not limited to packet capture rate and data retention period (e.g., 5% of the agency's traffic traversing the TIC Portal for a period of 60 days).

4. Custom Reports: The contractor shall provide reports as required by the ordering agency, including ad-hoc reports.
5. Agency NOC/SOC Console: The contractor shall provide additional features and functions customized to agency's specifications not covered by the Web portal included in the basic service.
6. Custom Security Assessment and Authorization Support (formerly known as Certification & Accreditation (C&A)): Agencies opting for security controls more stringent than the NIST High-Impact Baseline will negotiate agency-unique requirements directly with the contractor.
7. External Network Connection: The contractor shall enable the agency to connect to external IP networks at their physical locations. The traffic exchanged shall be IP traffic only and compliant to TIC portal's interconnecting requirements. The TIC portal shall support dedicated external connections to external partners (e.g., non-TIC federal agencies, externally connected networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but not limited to, permanent VPN over external connections, including the Internet, and dedicated private line connections to other external networks. The following baseline capabilities shall be supported for external dedicated VPN and private connections implemented using communication services offered through this contract, i.e. private lines or other dedicated connections SONETS, E-LINE, VPNS, etc. at the TIC portal:
   a) The connection shall terminate at an appropriate point so that traffic can be routed through the EINSTEIN Enclave to allow traffic to/from the external connections to be inspected. The EINSTEIN Enclave and the security stack at the portals are the public-facing side of the TIC Zone. The incoming traffic from the external network shall be inspected within the EINSTEIN Enclave and the security stack before reaching the internal network.
   b) The connection shall terminate in front of the full suite of TIC sensors/capabilities to allow traffic to/from external connections to be inspected.
   c) When connecting over the public networks including the Internet, the VPN connections shall be encrypted, compliant to NIST FIPS 140-2.
   d) Connections terminated prior to routing through the EINSTEIN Enclave may use split tunneling. If required by the agency, the MTIPS contractor shall configure telecommunications service priority (TSP) for external connections, including to the Internet, to provide for priority restoration of telecommunication services.

e) The External Network Connection Feature is subject to performance measures established by EIS depending on the transport service selected for connectivity and included in Sections C and Section J.

8. Encrypted DMZ: The contractor shall support encryption, FIPS 140-2 compliant, from the agency's SDP at the edge of the agency's WAN to the MTIPS Portal. The contractor shall provide encryption devices and shall manage the devices.

9. Remote Access: The MTIPS portal shall support remote access for teleworkers connecting from home or satellite offices and mobile, on-the-go workers. Teleworkers and mobile workers are a subscriber agency's authorized staff who connect via ad-hoc Virtual Private Networks (VPNs) through external connections, including the Internet. For permanent VPN connections for branch offices or business partners use Feature 7 or 10 as appropriate. In addition to supporting the requirements of OMB M-06-16, "Protection of Sensitive Agency Information," the following baseline capabilities shall be supported for telework/remote access at the MTIPS portal:

   a) The VPN connection shall terminate at an appropriate point prior to routing through the EINSTEIN Enclave and the full suite of TIC sensors/capabilities so that all outbound traffic to/from the VPN users to external connections, including the Internet, can be inspected within the EINSTEIN Enclave and the MTIPS portal security devices. In the case of outgoing traffic from the VPN users, the "Remote Access Enclave" shall connect to the aggregation devices located at the MTIPS transport interface before connecting to the portal's security stack and the EINSTEIN Enclave so that the outgoing traffic from the remote user/teleworker/mobile worker be inspected prior to reaching the Public Internet.
   b) The VPN connection shall terminate in front of MTIPS-managed security controls including, but not limited to, a firewall and IDPS to allow traffic to/from remote access users to internal networks to be inspected.
   c) All VPN connections shall be NIST FIPS 140-2 compliant.
   d) The telework VPNS shall not be capable of split tunneling (see NIST SP 800-46 Rev1). Any VPN connection that allows split tunneling is considered an external connection, and terminates in front of the EINSTEIN Enclave.
   e) The contractor shall use multi-factor authentication (see NIST SP 800-46 Rev1).
   f) VPN concentrators and Virtual-Desktop/Application Gateways (Remote Access Enclave) shall use hardened appliances and shall be maintained in a separate network security boundary depending on the contractor's implementation.

g) Should telework/mobile worker remote clients use GFP, the VPN connection may use access at the IP network-level and access through specific Virtual Desktops/Application Gateways.

h) If telework/mobile worker remote clients use non-GFP, the VPN connection shall only use access through specific Virtual Desktops/Application Gateways.

i) Implementation requirements:

   i. The contractor shall support TLS and/or IPSec VPNs to connect to the MTIPS portals. The contractor shall provide the end device client (agent) if required by the agency.

   ii. The contractor shall support VPN Encryption Algorithm compliant to FIPS 140-2, i.e., 128-bit AES.

   iii. Multi-factor authentication services shall be supported, they include passwords and Cryptographic Tokens or PIVs

   iv. At the portal, the contractor shall build a separate DMZ (Remote Access Enclave) for Remote Access services to secure VPN concentrators and the rest of the infrastructure required to provide the service, e.g., Application Gateways, Virtualized Infrastructure, etc.

The contractor shall also support customized remote access implementations for teleworkers and mobile workers to meet agency-specific requirements.

10. Extranet Connections: The TIC portal shall support dedicated extranet connections to internal partners (e.g., TIC federal agencies, closed networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but not limited to, permanent VPN over external connections, including the Internet, and dedicated connections to other internal networks provided by communication services offered through this contract. The following baseline capabilities shall be supported for extranet dedicated VPN and private line connections at the TIC Portal:

a) The connection shall terminate at an appropriate point before routing through the EINSTEIN Enclave and the full suite of TIC sensors/capabilities so that all outbound traffic to/from the extranet connections to external connections, including the Internet, is inspected within the EINSTEIN Enclave.

b) The connection shall terminate in front of the MTIPS-managed security controls including, but not limited to, a firewall and IDPS to allow traffic to/from extranet connections to internal networks, including other extranet connections, to be inspected.

c) VPN connections over shared public networks, including the Internet shall be NIST FIPS 140-2 compliant.

d) Split tunneling shall not be allowed. Any VPN connection that allows split tunneling is considered an external connection, and must terminate prior to routing through the EINSTEIN Enclave.

e) Implementation requirements:

   i. IPSec VPN from the fixed remote location (business partners, remote agency's sites, other agencies' sites, etc.) to the MTIPS portals.
   ii. Multi-Factor Authentication: Passwords, Cryptographic Tokens or PIV shall be supported.

   The contractor shall also support customized remote access implementations for extranet connections to meet agency-specific requirements.

11. Inventory/Mapping Service: The agency may request the MTIPS contractor to keep an inventory or a complete map of all networks connected to the MTIPS portal. The MTIPS contractor shall maintain a complete map, or other inventory, of all subscriber agencies' networks connected to the TIC access portal. The MTIPS contractor validates the inventory through the use of network mapping devices. Static translation tables and appropriate points of contact shall be provided to US-CERT on a quarterly basis, to allow in-depth incident analysis.

C.2.8.4.3 Interfaces

The contractor shall support the UNIs at the SDP to connect to MTIPS Transport POP, as follows:

1. SONET Access as defined in Section C.2.9.1.4
2. Ethernet Access as defined in Section C.2.9.1.4

C.2.8.4.4 Performance Metrics

The performance levels and AQL of KPIs for MTIPS in Sections C.2.8.4.4.1 through C.2.8.4.4.2 are mandatory unless marked optional.

C.2.8.4.4.1 Performance Metrics for TIC Portal

KPI	User Type	Performance Standard (Level/Threshold)	AQL	How Measured
Av(TIC Portal)	Routine Critical	99.5%	≥ 99.5%	See Note 1
Grade of Service (Failover Time)	Routine	1 minute	≤ 1 minute	See Note 2

KPI	User Type	Performance Standard (Level/Threshold)	AQL	How Measured
Grade of Service (Monitoring and Correlation	Routine	Real Time	≤ 4 hours 90% of the time	See Note 3
	Critical	Real Time	≤ 4 hours 99.9% of the time	
Grade of Service (Configuration/ Rule Change)	Routine	Within 5 hours for a Normal priority change	≤ 5 hours	See Note 4
		Within 2 hours for a Urgent priority change	≤ 2 hours	
EN (Firewall Security Event Notification)	Routine	Within 24 hours of a Low category event	≤ 24 hours	See Note 5
		Within 4 hours of a Medium category event	≤ 4 hours	
		Within 30 minutes of a High category event	≤ 30 minutes	
EN (Intrusion Detection/ Prevention Security Event Notification)	Routine	Within 24 hours of a Low category event	≤ 24 hours	See Note 5
		Within 10 minutes of a High category event	≤ 10 minutes	
Grade of Service (Virus Protection Updates and Bug Fixes)	Routine	Normal Priority Update 24 hours	≤ 24 hours	See Note 6
		Urgent Priority Update 2 hours	≤ 2 hours	

Notes:

1. The TIC Portal availability is calculated as a percentage of the total reporting interval time that all the TIC Portal components are operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Failover Time for the TIC Portal is the time that it takes to switch from one TIC Portal instance to another provided by the same contractor.
3. The GOS (Monitoring and Correlation) – The monitoring and correlation agents in the contractor's SOC shall detect a security event within 4 hours of its initiation at (a) 90% AQL for Routine, and (b) 99.9% AQL for Critical service levels. The monitoring and correlation systems shall provide real time fusion.
4. The GOS (Configuration/Rule Change) value represents the elapsed time between the configuration/change request and the change completion. The value is measured by logs/reporting. Changes are initiated and prioritized by the agency, or may be implemented in response to an event. Changes initiated by the contractor require agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency).
5. The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification to the agency. Events are categorized as follows:
   a) Low – Events in the Low category have a negligible impact on service. They include incidents that do not significantly affect network security, as well as minor hardware, software and configuration problems.
   b) Medium – Events in the Medium category have a more serious impact on service, and may indicate a possible security breach, threat or attack attempt. They may also cause the service to operate in a degraded state.
   c) High – Events in the High category represent violations that severely impact service and operations. They indicate a true compromise of network security. These events also include major hardware, software, and configuration problems, which should be immediately reported via email, or telephone, as specified by the agency.
6. The GOS (Virus Protection Updates and Bug Fixes) represents the time between the release of the virus protection updates and bug fixes (patches), and their deployment. This indicator ensures automatic and timely delivery of updates/bug fixes.

C.2.8.4.4.2 Performance Metrics for MTIPS Transport Collection and Distribution

KPI	User Type	Performance Standard (Level/Threshold)	(AQL	How Measured
Av(Port)	Routine	99.95%	≥ 99.95%	See Note 1
	Critical	99.995%	≥ 99.995%	

KPI	User Type	Performance Standard (Level/Threshold)	(AQL	How Measured
Latency (CONUS)	Routine	60 ms	≤ 60 ms	See Note 2
	Critical	50 ms	≤ 50 ms	
GOS (Data Delivery Rate)	Routine	99.95%	≥ 99.95%	See Note 3
	Critical	99.995%	≥ 99.995%	
Time to Restore	Without dispatch	4 hours	≤ 4 hours	
	With dispatch	8 hours	≤ 8 hours	
EN(Security Incident Reporting)	Routine	Near real time	≤ 30 min	See Note 4

Notes:

1. Port availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the port is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Latency is the average one-way time for IP packets to travel over the EIS core network. The Backbone Latency metric does not apply for DSL and Cable High Speed access methods.
3. Network packet delivery is a measure of IP packets successfully sent and received over the EIS core network.
4. Security incident reporting to DHS US-CERT must be performed in near real-time, congruent with NIST SP 800-61 Rev 2), not to exceed 30 minutes, from the time of detection.

C.2.8.4.5 MTIPS Security Requirements

The contractor shall ensure security requirements are met for the MTIPS as defined in the System Security Plan (see Section C.2.8.4.5.4), at a High impact level and shall support government security and authorization efforts. The contractor shall also support the government's efforts to verify that these standards are being met.

C.2.8.4.5.1 General Security Compliance Requirements

In providing services under this contract, the contractor shall be subject to all applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements. The contractor shall comply with Federal Information Security Management Act (FISMA) associated guidance and directives to include Federal Information Processing Standards (FIPS), NIST SP 800 series guidelines (available at: http://csrc.nist.gov/), GSA IT security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of government IT. Compliance references shall include:

- Federal Information Security Management Act (FISMA) of 2002; (44 U.S.C. Section 301. Information Security) available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
- Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.) available at: https://www.congress.gov/113/bills/s2521/BILLS-113s2521es.pdf.
- Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996," available at: https://www.fismacenter.com/clinger%20cohen.pdf.
- Privacy Act of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and contractors," August 27, 2004; available at: http://www.idmanagement.gov/.
- OMB Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended; available at: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/.
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies" (Available at: http://www.whitehouse.gov/omb/memoranda_2004).
- OMB Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors" (Available at https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf.)
- OMB Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors" (Available at

https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf.)

- OMB Memorandum M-14-03, “Enhancing the Security of Federal Information and Information Systems” (Available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.)
- FIPS PUB 199, “Standards for Security Categorization of Federal Information and Information Systems”
- FIPS PUB 200, “Minimum Security Requirements for Federal Information and Information Systems”
- FIPS PUB 140-2, “Security Requirements for Cryptographic Modules”
- NIST Special Publication 800-18 Revision 1, “Guide for Developing Security Plans for Federal Information Systems”
- NIST Special Publication 800-30 Revision 1, “Guide for Conducting Risk Assessments”
- NIST Special Publication 800-34 Revision 1, “Contingency Planning Guide for Federal Information Systems”
- IST SP 800-37 Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”
- NIST SP 800-39, “Managing Information Security Risk: Organization, Mission, and Information System View”
- NIST SP 800-41 Revision 1, “Guidelines on Firewalls and Firewall Policy”
- NIST SP 800-37 Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”
- NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems”
- NIST SP 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations”
- NIST SP 800-53A Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans”
- NIST SP 800-61 Revision 2, “Computer Security Incident Handling Guide”

- NIST SP 800-64, Revision 2, “Security Consideration in the System Developments Lifecycle”
- NIST SP 800-88 Revision 1, “Guidelines for Media Sanitization”
- NIST SP 800-128, “Guide for Security-Focused Configuration Management of Information Systems”
- NIST SP 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations”
- NIST SP 800-160 “Systems Security Engineering” dated November 2016
- NIST SP 800-161, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”
- Committee on National Security Systems (CNSS) Policy No. 12, National Information Assurance Policy for Space Systems Used to Support National Security Missions.
- Committee on National Security Systems Instruction 1253 (CNSSI No. 1253), Security Categorization and Control Selection for National Security Systems.

In addition to complying with the requirements identified in the government policies, directives and guides specified above, the contractor shall comply with the current GSA policies, directives and guides listed below (the current documents are referenced within the GSA IT Security Policy and are available upon request submitted to the GSA CO*)*:

- GSA Information Technology (IT) Security Policy, CIO P 2100.1(J).
- GSA Order CIO P 2181.1 “GSA HSPD-12 Personal Identity Verification and Credentialing Handbook”
- GSA Order CIO 2104.1, “GSA Information Technology (IT) General Rules of Behavior”
- GSA CIO P 1878.1, “GSA Privacy Act Program”
- GSA CIO P 1878.2A, “Conducting Privacy Impact Assessments (PIAs) in GSA”
- GSA IT Security Procedural Guide 01-01, “Identification and Authentication”
- GSA IT Security Procedural Guide 01-02, “Incident Response”
- GSA IT Security Procedural Guide 01-05, “Configuration Management”
- GSA IT Security Procedural Guide 01-07, “Access Control”
- GSA IT Security Procedural Guide 01-08, “Audit and Accountability Guide”

- GSA IT Security Procedural Guide 05-29, “IT Security Training and Awareness Program”
- GSA IT Security Procedural Guide 06-29, “Contingency Planning”
- GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk”
- GSA IT Security Procedural Guide 06-32, “Media Protection Guide”
- GSA IT Security Procedural Guide 07-35, “Web Application Security Guide”
- GSA IT Security Procedural Guide 08-39, “FY 2014 IT Security Program Management Implementation Plan”
- GSA IT Security Procedural Guide 10-50, “Maintenance Guide”
- GSA IT Security Procedural Guide 11-51, “Conducting Penetration Test Exercise Guide”
- GSA IT Security Procedural Guide 12-63, “GSA’s System and Information Integrity”
- GSA IT Security Procedural Guide 12-64, “Physical and Environmental Protection”
- GSA IT Security Procedural Guide 12-66, “Continuous Monitoring Program”
- GSA IT Security Procedural Guide 12-67, “Securing Mobile Devices and Applications Guide”
- GSA IT Security Procedural Guide 14-69, “SSL / TLS Implementation Guide”

C.2.8.4.5.2 Security Compliance Requirements

FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems,” is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in eighteen security-related areas. Contractor systems supporting the government must meet the minimum security requirements through the use of the security controls in accordance with NIST SP 800-53 Revision 4 (hereinafter described as NIST SP 800-53).

To comply with the federal standard, the government has determined the security category of the information and information system in accordance with FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems,” to be established at the High Impact Level and baseline security controls must be established as identified in NIST SP 800-53 and other associated directives and guides identified and/or provided by GSA. The contractor shall submit a Risk Management

Framework Plan describing its approach for MTIPS security compliance. This plan shall be submitted with the proposal in accordance with NIST SP 800-37. (Reference: NIST SP 800-37 R1, and NIST SP 800-53 R4: SA-3, RA-3)

C.2.8.4.5.3 Security Assessment and Authorization (Security A&A)

The implementation of a new federal government IT system requires a formal approval process known as security A&A. NIST SP 800-37 Revision 1 (hereinafter listed as NIST SP 800-37) and GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk", provides guidance for performing the A&A process. The contractor's system shall have a valid security A&A (approved by GSA) prior to being placed into operation and processing government information. Failure to obtain and maintain a valid security A&A will be grounds for termination of the contract. The system must have a new security A&A conducted (and approved by GSA) at least every three (3) years, or when there is a significant change that impacts the system's security posture, or a system may qualify for ongoing security authorizations that are not time-limited (at the discretion of the Authorizing Official (AO)). All NIST SP 800-53 controls must be tested and assessed no less than every three (3) years unless otherwise determined by the AO.

C.2.8.4.5.4 System Security Plan (SSP)

The contractor shall comply with all security A&A requirements as mandated by federal laws, directives and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The level of effort for the security A&A is based on the System's NIST FIPS Publication 199 categorization. At a minimum, the contractor shall create, maintain and update the following security A&A documentation:

1. The SSP shall be completed in accordance with NIST SP 800-18 Revision 1 (hereinafter listed as NIST SP 800-18) and other relevant guidelines. The SSP shall also include, at a minimum, the following appendices consisting of required policies and procedures across 18 control families mandated per FIPS 200. The SSP for the information system shall initially be completed and submitted within 30 days of the NTP to include annual updates (Reference: NIST SP 800-53 R4: PL-2).
2. The contractor shall develop and maintain a Security Assessment Boundary and Scope Document (BSD) as identified in NIST SP 800-37. This document will be used to determine the actual security assessment boundary. The set of information resources allocated to an information system defines the boundary for that system. These resources support the same mission/business objectives or functions. Generally the set of information resources is located within the

same operating environment; however, distributed systems can reside in various locations with similar operating environments. Establishing and/or changing information system security boundaries is a cooperative effort between the federal government and the industry partner(s). Key stakeholders within the federal government and its counterparts within the industry partner(s) include but are not limited to the following: Information System Owner, Chief Information Security Officer, Authorizing Official, and Information Systems Security Manager/Officer. A template is available in Section J.8. The BSD for the information system shall intially be completed and submitted within 15 days of the NTP to include annual updates (Reference: NIST SP 800-37 R1).

3. The contractor shall develop and maintain Interconnection Security Agreements (ISA) in accordance with NIST SP 800-47. The contractor shall provide any ISAs for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CA-3).
4. The contractor shall develop and maintain a GSA NIST SP 800-53 R4 Control Tailoring Workbook as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk”. A template is included in Section J.8. Column E of the workbook titled “Contractor Implemented Settings” shall document all contractor-implemented settings that are different from GSA-defined settings, and where GSA-defined settings allow a contractor to deviate. The contractor shall provide a Control Tailoring Workbook for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: AC-1).
5. The contractor shall develop and maintain a GSA NIST SP 800-53 R4 Control Summary Table for a High Impact Baseline as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” A template is provided in Section J.8. The contractor shall provide a GSA NIST SP 800-53 R4 Control Summary Table for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: AC-1).
6. The contractor shall develop and maintain a Rules of Behavior (RoB) for information system users as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk” and GSA Order CIO 2104.1, “GSA IT General Rules of Behavior”. The contractor shall provide an RoB for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: PL-4).
7. The contractor shall develop and maintain a System Inventory that includes hardware, software and related information as identified in GSA IT Security

Procedural Guide 06-30, “Managing Enterprise Risk”. The contractor shall provide a System Inventory for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CM-8).

8. The contractor shall develop and maintain a Contingency Plan (CP) including Disaster Recovery Plan (DRP) and Business Impact Assessment (BIA) completed in agreement with NIST SP 800-34. The contractor shall provide a CP for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CP-2).
9. The contractor shall develop and maintain a Contingency Plan Test Plan (CPTP) completed in agreement with GSA IT Security Procedural Guide 06-29, “Contingency Planning.” The contractor shall provide an CPTP for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CP-4).
10. The contractor shall test the CP and document the results in a Contigency Plan Test Report (CPTR), in agreement with GSA IT Security Procedural Guide 06-29, “Contingency Planning.” The contractor shall provide a CPTR for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CP-4).
11. The contractor shall perform a Privacy Impact Assessment (PIA) completed as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk”. The contractor shall provide a PIA for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: AR-2, AR-3 and AR-4).
12. The contractor shall develop and maintain a Configuration Management Plan CMP) (Reference: NIST SP 800-53 control CM-9; NIST SP 800-128; GSA CIO-IT Security 01-05). The contractor shall provide a CMP for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CM-9).
13. The contractor shall develop and maintain a System(s) Baseline Configuration Standard Document (Reference: NIST SP 800-53 control CM-2; NIST SP 800-128; GSA CIO-IT Security 01-05). The contractor shall provide a well defined, documented, and up-to-date specification to which the information system is built. The contractor shall provide the System Baseline Configuration for the information system as a part of the CMP with the initial security A&A package and provide annual updates (Reference: NIST SP 800-53 R4: CM-9).

14. The contractor shall develop and maintain System Configuration Settings (Reference: NIST SP 800-53 control CM-6; NIST SP 800-128; GSA CIO-IT Security 01-05). The contractor shall establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems shall be configured in accordance with GSA technical guides, NIST standards, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening systems, as deemed appropriate by the AO. System configuration settings shall be included as part of the CMP and shall be updated and/or reviewed on an annual basis (Reference: NIST SP 800-53 R4: CM-9).
15. The contractor shall develop and maintain an Incident Response Plan (IRP) (Reference: NIST 800-53 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02 “Incident Response”). The contractor shall provide an IRP for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: IR-8).
16. The contractor shall test the IRP and document the results in an Incident Response Test Report (IRTR) (Reference: NIST SP 800-53 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02 “Incident Response”). The contractor shall provide an IRTR for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: IR-3).
17. The contractor shall develop and maintain a Supply Chain Risk Management (SCRM) Plan. The contractor shall develop a SCRM Plan to reduce supply chain risks to performance and security of the contractor’s MTIPS throughout the contractor’s Muli-Agency TICAP solution life cycle. The contractor shall provide an SCRM Plan for the information system with its proposal to include annual updates (References: NIST SP 800-161 and NIST SP 800-53 R4: SA-12).
18. Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the contractor’s system and its environment of operation to determine if the security controls in the information system continue to be effective over time and as changes occur in the system and environment. The contractor shall develop and maintain a Continuous Monitoring Plan to document how continuous monitoring of information system will be accomplished. Through continuous monitoring, security controls and supporting deliverables shall be updated and submitted to GSA per the schedules below. The submitted deliverables provide a current understanding of the security state

and risk posture of the information systems. They allow GSA authorizing officials to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. The contractor shall provide a Continuous Monitoring Plan for the information system with the initial security A&A package followed by annual updates (Reference: NIST SP 800-53 R4: CA-7).

19. The contractor shall develop and maintain a Plan of Action and Milestones completed in agreement with GSA IT Security Procedural Guide 06-30, "Plan of Action and Milestones (POA&M)." All scans associated with the POA&M shall be performed as an authenticated user with elevated privileges. Vulnerability scanning results shall be managed and mitigated in the POA&M and submitted together with the quarterly POA&M submission. (Reference: NIST SP 800-53 R4; RA-5 and GSA CIO-IT Security Guide 06-30). Scans shall include all networking components that fall within the security accreditation boundary. The appropriate vulnerability scans shall also be submitted with the initial security A&A package. An annual information system User Certification/Authorization Review shall be annotated on the POA&M (a POA&M template is provided in Section J.8). The contractor shall provide a POA&M for the information system as part of the initial security A&A package followed by quarterly updates after receipt of the ATO. Note: Critical and High vulnerabilities shall be updated monthly (Reference: NIST SP 800-53 R4; CA-5).

20. All FIPS 199 Low, Moderate and High impact information systems must complete an independent internal and external penetration test and provide an Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities with security assessment package and on an annual basis in accordance with GSA CIO-IT Security Guide 11-51. GSA will provide for the scheduling and performance of these penetration tests. All penetration test exercises must be coordinated through the GSA Office of the Chief Information Security Officer (OCISO) Security Engineering (ISE) division at itsecurity@gsa.gov per GSA CIO-IT Security Guide 11-51. Applicable NIST SP 800-53 R4 Controls are CA-5 and RA-5.

21. All FIPS 199 Low, Moderate, and High impact information systems must conduct code analysis reviews in accordance with GSA CIO Security Procedural Guide 12-66 using the appropriate automated tools (e.g., Fortify, Veracode) to examine for common flaws, and document results in a Code Review Report to be submitted prior to placing system into production, when there are changes to code and on an annual basis. Applicable NIST SP 800-53, R4 Control is SA-11. References: GSA CIO Security Procedural Guides 06-30, "Managing Enterprise

Risk" and GSA CIO Security Procedural Guide 12-66, "Continuous Monitoring Program." If applicable, a Code Review Report shall be submitted as an initial deliverable prior to placing the information system into production, when there are changes to code, and on an annual basis (Reference: NIST SP 800-53 R4: SA-11).

22. The government is responsible for providing the Security/Risk Assessment and Penetration Tests. The contractor shall allow GSA employees (or GSA designated third party contractors) to conduct security A&A activities to include control reviews in accordance with NIST SP 800-53/NIST SP 800-53A and GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk". Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of government information. This includes the general support system infrastructure. All scans must be performed as an authenticated user with elevated privileges.
23. All identified gaps between required 800-53 controls and the contractor's implementation as documented in the Security/Risk Assessment Report (SAR) shall be tracked by the contractor for mitigation in a POA&M document completed in accordance with GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." Depending on the severity of the gaps, the government may require them to be remediated before an Authorization to Operate (ATO) is issued.
24. The contractor shall mitigate all security risks found during the security A&A and continuous monitoring activities. All critical and high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The government will determine the risk rating of vulnerabilities. Updates on the status of all critical and high vulnerabilities that have not been closed within 30 days shall be provided on a monthly basis.
25. The contractor shall deliver the results of the annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26, "FISMA Implementation". Each fiscal year the annual assessment will be completed in accordance with instructions provided by GSA (Reference: NIST SP 800-53 R4: CA-2).
26. Systems normally fall under the three (3) year security reauthorization process; however, a system may qualify for ongoing security authorizations that are not time-limited as per OMB M-14-03. To qualify for non-time limited authorizations,

acceptance into the GSA Continuous Monitoring Program will be in accordance with GSA CIO Security Procedural Guide 12-66 “Continuous Monitoring Program” and NIST SP 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations.” If the system is accepted under the GSA Continuous Monitoring Program by the GSA AO, the contractor shall provide the following deliverables to the GSA COR/ISSO/ISSM on a monthly basis in accordance with GSA COI Security Procedural Guide 12-66:

a) Reports on SCAP Common Configuration Enumerations (CCE) (NIST SP 800-53 R4: CM-6)
b) Reports on SCAP Common Platform Enumeration (CPE) (NIST SP 800-53 R4: CM-8)
c) Reports on SCAP Common Vulnerabilities and Exposures (CVE) (NIST SP 800-53 R4: CM-8)

27. The contractor shall develop and keep current all policy and procedures documents, as outlined in the specified NIST documents as well as appropriate GSA IT Security Procedural Guides. The following documents shall be verified and reviewed during the initial security assessment and updates provided to the GSA COR/ISSO/ISSM biennially:

a) Access Control Policy and Procedures (NIST SP 800-53 R4: AC-1)
b) Security Awareness and Training Policy and Procedures (NIST SP 800-53 R4: AT-1)
c) Audit and Accountability Policy and Procedures (NIST SP 800-53 R4: AU-1)
d) Security Assessment and Authorization Policies and Procedures (NIST SP 800-53 R4: CA-1)
e) Configuration and Management Policy and Procedures (NIST SP 800-53 R4: CM-1)
f) Contingency Planning Policy and Procedures (NIST SP 800-53 R4: CP-1)
g) Identification and Authentication Policy and Procedures (NIST SP 800-53 R4: IA-1)
h) Incident Response Policy and Procedures (NIST SP 800-53 R4: IR-1)
i) System Maintenance Policy and Procedures (NIST SP 800-53 R4: MA-1)
j) Media Protection Policy and Procedures (NIST SP 800-53 R4: MP-1)
k) Physical and Environmental Policy and Procedures (NIST SP 800-53 R4: PE-1)
l) Security Planning Policy and Procedures (NIST SP 800-53 R4: PL-1)
m) Personnel Security Policy and Procedures (NIST SP 800-53 R4: PS-1)

n) Risk Assessment Policy and Procedures (NISTSP 800-53 R4: RA-1)
o) Systems and Services Acquisition Policy and Procedures (NIST SP 800-53 R4: SA-1)
p) System and Communication Protection Policy and Procedures (NIST SP 800-53 R4: SC-1)
q) System and Information Integrity Policy and Procedures (NIST SP 800-53 R4: SI-1)

C.2.8.4.5.5 Additional Security Requirements

The contractor shall ensure that proper privacy and security safeguards are adhered to in accordance with the FAR Part 52.239-1, see Section I.

The deliverables identified in Section **Error! Reference source not found.** shall be labeled "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) or contractor selected designation per document sensitivity. External transmission/dissemination of Controlled Unclassified Information (CUI) data to or from a GSA computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "*Security requirements for Cryptographic Modules.*"

Where appropriate, the contractor shall ensure implementation of the requirements identified in the FAR (see Section I, 52.224-1, "*Privacy Act Notification*" and FAR 52.224-2, "*Privacy Act*.")

The contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the federal government's agent.

The government has the right to perform manual or automated audits, scans, reviews, or other inspections of the contractor's IT environment being used to provide or facilitate services for the government. In accordance with the FAR (see Section I, 52.239-1) the contractor shall be responsible for the following privacy and security safeguards:

1. The contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the contractor under this contract or otherwise provided by the government (except for disclosure to a consumer agency for purposes of security A&A verification).
2. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the confidentiality, integrity and availability of any non-public government data collected and stored by the contractor. The contractor shall afford the government logical and physical access to the contractor's facilities, installations, technical capabilities, operations, documentation, records,

and databases within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods:

- Authenticated and unauthenticated operating system/network vulnerability scans;
- Authenticated and unauthenticated web application vulnerability scans;
- Authenticated and unauthenticated database application vulnerability scans and
- Internal and external penetration testing.

3. Automated scans can be performed by government personnel, or agents acting on behalf of the government, using government operated equipment, and government specified tools. If the contractor chooses to run its own automated scans and/or penetration tests, results from these scans and/or penetration tests may, at the government's discretion, be accepted in lieu of government performed vulnerability scans and/or penetration tests. In these cases, scanning tools and their configurations shall be approved by the government. In addition, the results of contractor-conducted scans and/or penetration tests shall be provided, in full, to the government.

C.2.8.4.5.5.1 Personnel Background Investigation Requirements

The contractor shall perform personnel security / suitability checking in accordance with FAR Part 52.204-9 (see Section I).

All contractor personnel with access to the contracted system that is within the security A&A scope must successfully complete a background investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12), OMB guidance M-05-24, M-11-11, and as specified in GSA CIO Order 2100.1J and GSA Directive 9732.1D Suitability and Personnel Security to provide services under this contract. The required background investigations for administrative personnel shall be a minimum of a National Agency Check with Written Inquiries (NACI) and for technical staff shall be a Minimum Background Investigation (MBI) or higher depending upon their access and control over the systems. GSA will pay for any required background investigations for MTIPS.

C.2.8.5 Managed Security Service

C.2.8.5.1 Service Description

The array of services and technologies in the IT arena continues to expand as users and applications are added to agency networks. At the same time, cybercriminals and corrupt organizations are becoming ever more mobile and sophisticated. Therefore,

agencies will continue to need managed security services to safeguard agency internal networks and systems against ever-evolving security threats.

Managed security services provide protection of endpoints, email, web, and networks, and include capabilities such as authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management.

C.2.8.5.1.1 Functional Definition

MSS comprises the following underlying functions:

1. Managed Prevention Service
2. Vulnerability Scanning Service
3. Incident Response Service

These functions are described below:

Managed Prevention Service (MPS) provides the ability to monitor hosts and network traffic, and analyze network protocol and application activity to identify and mitigate suspicious activity. Supporting capabilities include managed firewalls, host- and network-based threat mitigation, as well as email- and DNS-based threat mitigation services.

Vulnerability Scanning Service (VSS) searches for security holes, flaws, and exploits on agency systems, networks and applications. The service tests for vulnerabilities by comparing scanned information to data contained in a database, which is updated as new threats are discovered. VSS can also simulate a real intrusion in a controlled environment, in order to gauge a network's susceptibility to attacks. The service performs external scans by remotely probing a network for vulnerabilities that generally come from the outside; and internal scans which detect flaws originating from the inside.

Incident Response Service (INRS) is comprised of both proactive and reactive activities. Proactive services are designed to prevent incidents. They include onsite consulting, strategic planning, security audits, policy reviews, vulnerability assessments, security advisories, and training. Reactive services involve telephone and on-site support for monitoring and analyzing alert information and responding to malicious events such as Denial of Services (DoS) attacks; virus, worm, and Trojan horse infections; illegal inside activities, espionage, and compromise of sensitive internal agency databases. INRS provides an effective method of addressing these security intrusions, thereby ensuring operational continuity in case of attacks. In addition, INRS provides forensics services that can assist in apprehending and prosecuting offenders.

C.2.8.5.1.2 Standards

MSS shall comply, at a minimum, with the following standards:

1. FISMA (44 U.S.C. Section 301. Information security) available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
2. NIST FIPS PUB 140-2 – Security Requirements for Cryptographic Modules
3. NIST FIPS PUB 199 – Standards for Security Categorization of Federal Information and Information Systems
4. NIST SP 800-40 – Guide to Enterprise Patch Management Technologies
5. NIST SP 800-41 – Guidelines on Firewalls and Firewall Policy
6. NIST SP 800-45 – Guidelines for Electronic Mail Security
7. NIST SP 800-51 – Guide to Using Vulnerability Naming Schemes
8. NIST SP 800-61 – Computer Security Incident Handling Guide
9. NIST SP 800-81-2 – Secure Domain Name System (DNS) Deployment Guide
10. NIST SP 800-83 – Guide to Malware Incident Prevention and Handling for Desktops and Laptops
11. NIST SP 800-92 – Guide to Computer Security Log Management
12. NIST SP 800-94 – Guide to Intrusion Detection and Prevention Systems
13. NIST SP 800-122 – Guide to Protecting the Confidentiality of Personally Identifable Information (PII)
14. NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
15. NIST Interagency Report 7802 – Trust Model for Security Automation Data (TMSAD) Version 1.0
16. United States Computer Emergency Readiness Team (US-CERT) reporting requirements
17. IETF - Request for Comments (IETF-RFC) 2350 Expectations for Computer Security Incident Response
18. All new versions, amendments, and modifications of the above
19. All appropriate standards for any applicable underlying EIS access and transport services

C.2.8.5.1.3 Connectivity

MSS shall connect to and interoperate with the agency networking environment, including Demilitarized Zones (DMZs) and secure LANs, as required by the agency. The service shall also support connectivity to extranets and the Internet.

C.2.8.5.1.4 Technical Capabilities

The MSS capabilities, as defined in the following Sections C.2.8.5.1.4.1 through C.2.8.5.1.4.3 are mandatory unless marked optional.

C.2.8.5.1.4.1 Managed Prevention Service (MPS)

1. The contractor shall provide design and implementation services. This will enable the agency and the contractor to discuss matters such as system recommendations, a baseline assessment, rules, signature sets, configurations, and escalation procedures.
2. The contractor shall provide software and hardware components, including log servers, as applicable.
3. The contractor shall implement hardware or software load balancing capabilities and redundancy necessary to meet KPI and agency requirements.
4. The contractor shall provide installation support to include testing of equipment, testing of software, and loading of any agency-relevant data, as required by the agency.
5. The contractor shall maintain the latest configuration information for restoration purposes, reporting, and forensics analysis.
6. The contractor shall maintain the managed service capabilities, performing hardware/software upgrades and replacements, and content updates.
7. The contractor shall ensure that MPS systems and components comply with NIST SP 800-53 identification and authentication controls for high impact systems (FIPS 199). Administrative access devices requires multi-factor authentication (OMB M-11-11).
8. The contractor shall notify the agency about patches and bug fixes as soon as they become available.
9. The contractor shall test and deploy the latest patches and bug fixes as soon as they become available and are approved by the agency.
10. The contractor shall perform and document configuration and management as applicable to ensure that security, access, and information-flow policies are enforced as requested by the agency.
11. The contractor shall proactively monitor the health and status of MPS hardware/software components on a 24x7 basis for indications of compromise such as intrusions, anomalies, malicious activities, and network misuse.
12. The contractor shall monitor the overall performance of the service, including the adequacy of the hardware/software components as the network expands.
13. The contractor shall ensure the service allows only necessary functionality, network protocols, ports or services with documented customer approval.

14. The contractor shall perform and document periodic validation activities (e.g., via scans) to ensure service configurations are not vulnerable and are enforcing agency policies.
15. The contractor shall notify the agency of MPS-failure events via email, fax, or telephone, as directed by the agency.
16. The contractor shall be able to receive, handle, and use sensitive but unclassified cybersecurity indicators provided by the agency or the Department of Homeland Security (DHS).
17. The contractor shall ensure that service statistics, events messages, logs, and suspected attack information are sent via secure means to the agency-specified operation center.
18. The contractor shall ensure that event messages associated with DHS-provided indicators are sent via secure means to DHS.
19. The contractor shall ensure that event messages have necessary and consistent timestamps and content to establish context including, as appropriate, date/time of occurance (including time zone); related indicators, policies, and anomalies; source and destination addresses, ports, and protocols; operating system, processes, and application; detection source and location.
20. The contractor shall be able to identify and retrieve each customer agency's data for the agency, without divulging any other agency's data.
21. The contractor shall provide the agency with secure web access to logs and service information including the following:
    a) Active Sessions
    b) Port and Protocol Activity
    c) Authentication Statistics
    d) Connections/Attempts counts and results (accepted/rejected) by port
    e) Events, rule violations, and attacks detected including name,description, level, impact date, time, vulnerabilities and targeted weakness, and remedies
    f) Source and Destination IP Addresses, domains (fully-qualified domain name) and URLs; as well as statistics
    g) Affected endpoints
    h) Managed Prevention Service Statistics and Utilization
    i) Outages
    j) Configuration Modifications
    k) Change Requests and Event Tickets

C.2.8.5.1.4.2 Vulnerability Scanning Service (VSS)

The contractor shall support the agency in establishing, implementing and maintaining a vulnerability scanning service, which shall be operational on a 24x7 basis. The service shall provide the following:

1. External Vulnerability Scanning which tests Internet-connected nodes in the network, including web environments.
2. Internal Vulnerability Scanning which looks for local/host flaws and internal threats, usually inside the firewall.

The service shall periodically probe networks, including operating systems and application software, for potential openings, security holes, and improper configuration.

The service shall probe agency systems for vulnerabilities in, but not limited to, the following areas:

1. Back doors
2. Bind
3. Browser
4. Brute Force Attacks
5. Common Gateway Interface - Binary (CGI-Bin)
6. Daemons
7. Distributed Component Object Model (DCOM)
8. Databases
9. Domain Name Service (DNS)
10. eCommerce Applications
11. Email
12. Firewalls
13. File Sharing
14. FTP
15. General Remote Services
16. Hardware and Network Appliances
17. Hubs
18. Information/Directory Services
19. Instant Messaging
20. Lightweight Directory Access Protocol (LDAP)
21. Mail Applications
22. Multimedia Internet Mail Extension (MIME)

23. Network
24. Network Sniffers
25. Netbios
26. Network File System (NFS)
27. Network Information System (NIS)
28. OS Critical Issues
29. OS Groups
30. OS Networking
31. OS Password Checks
32. OS Policy Issues
33. OS Registry
34. OS Services
35. OS Users
36. Port Scans
37. Protocol Spoofing
38. Router-Switch
39. Remote Procedure Call (RPC)
40. Shares
41. Simple Mail Transfer Protocol (SMTP)
42. Simple Network Management Protocol (SNMP)
43. Server Message Block (SMB)
44. Transmission Control Protocol / Internet Protocol (TCP/IP)
45. Trojan Horses
46. Web Scans
47. Web Servers
48. Wireless Access Points

The contractor shall:

1. Proactively identify network vulnerabilities and propose appropriate countermeasures, fixes, patches, and workarounds.
2. Notify the agency of vulnerabilities discovered via email, fax, or telephone, as directed by the agency.
3. Provide the agency with secure Web access to vulnerability information, scan summaries, device/host reports, and trend analyses.

4. Review vulnerabilities discovered with the agency, as required.
5. Provide scan scheduling flexibility to the agency in order to minimize any interruptions in normal business activities.
6. Provide the agency with non-destructive and non-intrusive vulnerability scans that will not crash the systems being analyzed or disrupt agency operations. The scans shall not provoke a denial of service condition on the agency system being probed.
7. Use other analytical means to ascertain the vulnerability of agency systems if a particular scan is potentially destructive or intrusive.
8. Ensure that the scanning engine is regularly updated with new vulnerabilities information in order to maintain effectiveness of the service.
9. Support networks of varying size and complexity.

C.2.8.5.1.4.3 Incident Response Service (INRS)

1. The contractor shall review the agency's security infrastructure and develop appropriate strategic plans in collaboration with the agency. These plans shall detail the incident response process, identify internal resources, assign duties to team members, describe policies, define severity levels, list escalation chains, and specify emergency/recovery procedures.
2. The contractor shall provide the agency with effective incident response support on a 24x7 basis.
3. The contractor shall maintain a problem detection system for the diagnosis of alerts and violations.
4. The contractor shall analyze suspicious security alerts to determine the significance and scope of an event and immediately notify the agency when the event is deemed high priority.
5. The contractor shall provide the agency with immediate access to vulnerability and severe alert information, which shall contain but not be limited to the following: Description, Target, Origin, Potential Incident Impacts, Remedies, Prevention Measures.
6. The contractor shall coordinate with the agency to handle potential security incidents according to the appropriate response procedures.
7. The contractor shall provide countermeasures to contain the security incident, limit its spread, and protect internal systems.
8. The contractor shall recommend the fixes necessary to eliminate identified vulnerabilities, and appropriate procedures to guard against future attacks.
9. The contractor shall provide the agency with secure web access to incident analysis findings and recommendations.

10. The contractor shall assist the agency in containing the damage and restoring affected systems to their normal operational state.
11. The contractor shall assist the agency in testing restored systems in order to ensure that identified vulnerabilities have been corrected.
12. The contractor shall provide dedicated support until resolution of the problem.
13. The contractor shall provide post-incident investigative and forensics services. This includes isolating the impacted area, capturing and collecting data, categorizing malicious or illegal events, and performing reconstruction analyses. The contractor shall handle and preserve the data collected according to sound scientific and evidence rules, as the information may serve as evidence in administrative actions and legal proceedings. The contractor shall trace the offenders and assist in prosecuting attackers, as required.
14. The contractor shall provide telephone support to the agency, as required.
15. The contractor shall deploy cybersecurity personnel to agency sites to handle security incidents, as necessary.
16. The contractor shall provide security awareness training to agency personnel as required. This includes mock attack drills, emerging threats and vulnerabilities workshops, and new incident response tools and processes demonstrations. The frequency and nature of training activities may vary according to agency needs.

C.2.8.5.2 Features

The following MSS features are mandatory unless marked optional.

1. Managed Prevention Service:
    a) Firewall – The contractor shall provide, operate and manage hardware and software components to analyze packet headers and enforce policy based on protocol type, source address, destination address, source port, and/or destination port. The managed firewall solutions shall apply stateful protocol analysis to compare traffic to generally accepted definitions of benign protocol activity and identify deviations. The firewall will provide Network Address Translation (NAT) and Port Address Translation (PAT) in order to disguise internal IP addresses, and it shall enforce agency-specified security policies by blocking packets and terminating sessions that violate those policies.
    b) Personal Firewalls – The contractor shall provide personal firewalls or personal firewall appliances in order to secure remote personal computers or small remote networks (i.e., home offices), as required by the agency
    c) Network Intrusion Prevention System – The contractor shall provide an in-line deep-packet capability to monitor network traffic (HTTP/S, FTP, etc.), analyze network and application protocol activity and content to identify and mitigate

suspicious activity, and block or disrupt activity based on signatures and behavor.

d) Endpoint Protection – The contractor shall provide host-based intrusion prevention capabilities, including application firewall, endpoint recording, threat detection, whitelisting, banning, and remediation in order to protect agency endpoints.

e) Secure Web Proxy – The contractor shall provide an intermediary between endpoints allowing URL- and domain-based filtering as well as obfuscation of internal IP addresses. The contractor shall support URL blocking.

f) Inbound Web Filtering – The contractor shall provide the ability to filter inbound web sessions to web servers at the HTTP/HTTPS/SOAP/XML-RPC/Web Service application layers from, but not limited to, cross site scripting (XSS), SQL injection flaws, session tampering, buffer overflows and malicious web crawlers.

g) Application-Level Gateway – The contractor shall provide an intermediary between endpoints allowing for application layer control/data protocols (FTP, SIP, IM, etc.) to be proxied.

h) Network Behavior Analysis – The contractor shall provide a capability that develops a profile of 'normal' agency behavior and examines network traffic (including encrypted sessions) to identify threats that generate unusual traffic flows, such as DDoS attacks, scanning, and certain forms of malware. The contractor shall perform anomaly detection in order to identify atypical traffic trends and unusual behaviors that may indicate a potential attack. The contractor shall keep logs of at least the source, destination and size of the encrypted connections for further analysis.

i) Network Traffic Content Analysis and Sandboxing – The contractor shall provide capabilities that extract objects from network traffic and examine those objects using real-time binary and execution engine analysis.

j) Email Forgery Protection and Filtering – The contractor shall provide capabilities for inbound and outbound forgery protection (domain-level sender forgery analysis equivalent to Domain Keys Identified Mail or Sender Policy Framework standards, digital signing procedures for outgoing email messages to ensure that they have been digitally signed at the domain level), as well as domain and header-based filtering, phishing and spam filtering, block attachments violating policy (e.g., size, file type), sanitize malicious content and quarantine messages, as well as measures that can conceal, limit, or change information about the agency's networks or domains, reducing visibility to outsiders.

k) Email Content Analysis and Sandboxing – The contractor shall provide capabilities that extract objects from email traffic and examine those objects using real-time binary and execution engine analysis.

l) User Authentication Integration - The contractor shall support the integration of the email-based threat mitigation service with the agency's own authentication service, as specified by the agency. Examples include Kerberos, Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory, Remote Authentication Dial-In User Service (RADIUS),RSA SecureID, Terminal Access Controller Access Control System (TACACS), Extended TACACS (XTACACS), or TACACS+.

m) DNSSEC – The contractor shall provide DNS security capabilities described in NIST SP800-81-2 to ensure data integrity and source authentication.

n) DNS Sinkholing – The contractor shall provide capabilities to block or redirect network traffic based on manipulation of DNS query responses.

o) Data Loss Prevention – The contractor shall provide capabilities to discover and identify sensitive data and to manage, monitor, and protect it from being deleted, destroyed or divulged.

p) Demilitarized Zones (DMZs) Support – The contractor shall support connections to Demilitarized Zones (DMZs) which serve as buffers between the agency's private networks and outside public networks. DMZs can apply to Web (HTTP), FTP, email (SMTP), and DNS servers.

q) Extranet Support – The contractor shall support connections to extranets which can facilitate inter-agency interactions or enable the agency to interface with trusted stakeholders.

r) Firewall-to-Firewall VPNs – The contractor shall support firewall-to-firewall VPNs which establishes secure tunnels between agency firewalls, and also between firewalls and the contractor's operation center.

s) Remote Client VPNs – The contractor shall provide remote agency users with secure access to the network, employing VPN encryption technology.

t) EINSTEIN 2 – The contractor shall interact with DHS to obtain indicators, establish USCERT event feeds, and provide EINSTEIN network flow and detection capabilities for agency-specified traffic.

u) Short-Term Storage – The contractor shall provide storage capacity to retain at least 24 hours of agency-specific data generated by the MPS. Traffic shall be selectively filtered and stored, and retained data shall be made securely available to the agency.

v) Long-Term Storage – The contractor shall provide storage capacity to retain a year of agency-specific data generated by the MPS. Traffic shall be selectively filtered and stored, and retained data shall be made securely available to the agency.

w) Agency-specified policy enforcement.

2. Vulnerability Scanning Service (VSS):

   a) VSS API: The contractor shall provide the agency with the ability to integrate the service into its own tools and applications, using for example, a standard XML and RESTful APIs, as required by the agency. This will assist in-house security personnel with tasks such as scanning IP addresses, assessing host vulnerabilities, creating user accounts, and exporting vulnerability data.

3. Incident Response Service (INRS)

   a) Advanced Analytics. The contractor shall provide and apply various statistical techniques from the modeling, machine learning, and data mining disciplines to analyze relevant observations for threat discovery, assessment, situational awareness, and prediction. Where applicable, the techniques provided must yield confidence intervals establishing the statistical significance of findings. When statistical significance cannot be established using rigorous, state-of-the-art techniques, the findings must include this caveat.

C.2.8.5.3 Interfaces

MSS shall support the following services:

1. VPNS as specified in Section C.2.1.1.1
2. ETS as specified Section C.2.1.2
3. IPS as specified in Section C.2.1.7

C.2.8.5.4 Performance Metrics

The MSS performance levels and AQL of KPI in Section C.2.8.5.4.1 are mandatory unless marked optional.

C.2.8.5.4.1 Managed Security Service Performance Metrics

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Event Notification (EN) for MPS	Routine	Within 10 minutes	≤ 10 minutes	
Event Notification (EN) for INRS	Routine	Next business day or within 24 hours for a Low category event	≤ Next business day or 24 hours	See Note 2

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
		Within 4 hours of a Medium category event	≤ 4 hours	
		Within 1 hour of a High category event	≤ 1 hour	
Grade of Service (Configuration Change, Virus Protection Updates)	Routine	Within 5 hours (for MPS) and 24 hours (for VSS) for a Normal priority change	≤ 5 hours (MPS) and ≤ 24 hours (VSS)	See Note 3
		Within 2 hours for an Urgent priority change	≤ 2 hours	
Incident Response Time (Telephone)	Routine	Within 1 hour of the notification for a Low category incident	≤ 1 hour	See Note 4
		Within 15 minutes of the notification for a High category incident	≤ 15 minutes	
Incident Response Time (On-Site)	Routine	Within 36 hours of the notification for a Low category incident	≤ 36 hours	See Note 5
		Within 24 hours of the notification for a High category incident	≤ 24 hours	
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. MSS availability is calculated as a percentage of the total reporting interval time that the MSS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification of the agency. Events are categorized as follows:
   a) Low — Events in the Low category have a negligible impact on service. They include firewall incidents that do not significantly affect network security, as well as minor hardware, software and configuration problems.
   b) Medium — Events in the Medium category have a more serious impact on service, and may indicate a possible security breach, threat or attack attempt. They may also cause the service to operate in a degraded state.
   c) High — Events in the High category represent firewall violations that severely impact service and operations. They indicate a true compromise of network security. These events also include major hardware, software and configuration problems, and are immediately reported via email or telephone, as specified by the agency.
3. The Grade of Service (Configuration Change) value represents the elapsed time between the configuration change request and the change completion. Changes are initiated and prioritized by the agency, or may be implemented in response to an event. Changes initiated by the contractor require agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency). Exceptions may be associated with agency-specified and agreed-upon maintenance windows that require pre-planned integration.
4. The Telephone Incident Response value represents the elapsed time between the agency's notification to the contractor and the contractor's implementation of response procedures. These procedures, and what constitutes Low and High incidents, are defined in the TO.
5. The On-Site Incident Response value represents the elapsed time between the agency's notification to the contractor and the contractor's arrival to the affected site for implementation of response and investigative procedures. These procedures, and what constitutes Low and High incidents, are defined in the TO.

C.2.8.6 Managed Mobility Service

C.2.8.6.1 Service Description

Managed Mobility Service (MMS) helps agencies manage the transition to a more complex mobile computing and communications environment by supporting security, network services, and software and hardware management for mobile handheld

devices. This is especially important as Bring Your Own Device (BYOD) initiatives and advanced wireless computing become the focus of many agencies.

MMS is a core capability for effectively scaling the secure deployment and management of mobile applications, enterprise data on mobile devices, and management of the devices and mobile platforms themselves. The optimal balance between security, total costs and functionality will provide the most business value to the agencies.

MMS may be offered as a cloud-based, premises-based, or hybrid solution.

C.2.8.6.1.1 Functional Definition

MMS supports mobile computing by allowing agency-owned and personal mobile handheld devices (smartphones and tablets, based on smartphone OSs) to access agency networks and applications in accordance with the agency's IT security policy. MMS supports mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), mobile security and deployment support.

C.2.8.6.1.2 Standards

MMS shall comply with the following standards:

1. FISMA Moderate Impact level or higher
2. NIST SP 800-53 Moderate
3. FIPS 140-2
4. IPv4 and IPv6
5. The specific standards, as identified in the TO

C.2.8.6.1.3 Connectivity

MMS shall interoperate with:

1. 3G/4G Cellular Service, based on standards for CDMA, GSM, and LTE
2. Smartphones and Tablets, based on smartphone OSs
3. Wi-Fi

C.2.8.6.1.4 Technical Capabilities

MMS capabilities are subdivided into MDM, MAM, MCM, Mobile Security, and Deployment Support, which are described in the following subsections.

C.2.8.6.1.4.1 Mobile Device Management (MDM)

MDM supports device management and other mobile management functions including operations, policy, security, configuration, mobile network performance, application

support (application performance, version control, distribution, etc.), mobile data management (on device), and some mobile network monitoring.

The following capabilities are mandatory unless marked optional:

1. MDM capabilities include, but are not limited to, the following:
   a) Enforce enterprise rules while allowing agency/bureau/sub-bureau/etc. enrollment, reporting, management, and compliance activities.
   b) Take the following action upon a group of devices from a search: Reassign to Group (any type of logical grouping, e.g., user or device groupings).
   c) Assign Profile to one or many Groups (any type of logical grouping). User or device groupings are an example.
   d) View required applications from a Mobile Application Store (MAS).
   e) View and run reports on user and device information for all Smartphones including usage and cost.
   f) Run reports by groups of users to include location.
   g) Support a Software Development Kit (SDK) or API Framework to integrate with existing or future agency applications.
   h) Monitor the MDM system via industry standard tools.
   i) Integrate certificates from the MDM system's internal PKI system to mobile devices as well as third party public PKI providers.
   j) Perform MDM functions from within a secure VPN used to transport all enterprise/agency data (i.e.: no MDM control data is transported unencrypted across the open Internet).
2. Device Enrollment – adding a device to the MDM management domain:
   a) Set a Target Platform (Apple, Android, etc.) for profile provisioning.
   b) Use a Target Device Model for profile provisioning.
   c) Specify minimum OS version for profile provisioning.
   d) Use Target Device Ownership (GFP, personal, etc.) for profile provisioning.
   e) Allow a user to edit any field for a "live" or "active" profile.
   f) Allow a user with appropriate authorization to self-enroll an agency GFP or BYOD device.
   g) Centrally manage multiple devices for a single user (user device view).
   h) Support different policies or grouping for multiple devices under one user (i.e.: tablet policy, smartphone policy).

i) Apply multiple policies to devices simultaneously (user is member of group policy X, with device policy Y) – when multiple controls conflict, the most restrictive control takes precedence.
j) Use external directory service repository for enrollment.
k) Use federated (i.e., SAML) and multi-factor authentication for enrollment and restrict enrollment based on directory-based security groups
l) Set support email and phone information for registration messages.
m) Redirect users to a URL upon successful enrollment.
n) Edit an enrollment activation notification message to the user (email and/or SMS).
o) Set a default Device Ownership type upon enrollment for different groups.
p) Use an internal user list for enrollment for different groups.
q) Set support email and phone information for registration messages for different groups.
r) Edit an enrollment activation notification message to the user or group of users (email and/or SMS).
s) Send a user or group an activation enrollment message (email or SMS).

3. Device Profiles (per-user and per-group):

a) Create a profile template.
b) Copy profiles.
c) Edit a "live" or "active" profile.
d) Set Profile Removal Permission (who can remove a profile from a device or user).
e) Set Profile Start Date (when the profile starts applying to associated devices).
f) Set Profile End Date (when the profile stops applying to associated devices).
g) Automatically update a device that currently has a profile when editing that profile, and set Profile Geofences (profiles are active/inactive depending on physical device location).
h) Push a profile to any individual device.
i) Automatically remove profiles from devices whose state changes from qualifying to not-qualifying. This may happen as a result of changing a profile to be more exclusive.
j) Support multiple profiles being applied to a single device (most restrictive rules apply).

k) Delete a profile from the MDM system.
l) Set a description for a profile.
m) Manage the following via a profile:
    i. Install applications
    ii. Control use of camera
    iii. Control use of installed applications, including default applications
    iv. Allow multiple Wi-Fi configurations for multiple profiles
    v. Manage device Wi-Fi settings via a MDM policy
    vi. Control Wi-Fi Security Type: None, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA/WPA2), Enterprise/agency-specific (any)
    vii. Multiple VPN configurations for a single profile
    viii. VPN Connection (or Policy) Type: IPSec and TLS
    ix. VPN connection Proxy for a VPN configuration
    x. Multiple email/calendar/contact configurations per profile
    xi. Multiple Web Clip / Web Shortcut configurations per profile

4. Device Feature Management:
    a) Multi-OS Support – Manage multiple OS devices.
    b) Device passcode enforcement (complexity, length, presence).
    c) Installation of applications (See MAM)
    d) Camera (enable/disable).
    e) Control radios/communications:
        i. Wi-Fi (enable/disable)
        ii. Bluetooth (enable/disable)
        iii. Enable or disable specific hardware component and uses, such as enable Bluetooth headphone, disable Bluetooth keyboard
        iv. Near Field Communication (NFC) (enable/disable)
        v. GPS (enable/disable)
        vi. Store enterprise/agency data to removable media (disable)
5. Data Management – read, write, transmit and receive data on mobile devices as well as with backend systems/repositories:
    a) File Management – to secure data, files, and applications (e.g., pdf files or Word docs) on a mobile device
    b) Personal Information Management – mail, calendar, and address book capabilities

6. NIST SP 800-126 Security Content Automation Protocol (SCAP) support for the server-side components, including asset management, configuration management, patch management and remediation capabilities.
7. Device Inventory Management and Reports – to provision, control and track devices connected to corporate/agency applications and data, and to relate this data to user information, in accordance with the TO. Device Inventory Reports include all data associated with the device, OS and applications.
8. System Performance Reports – include key performance data to provide insight into the reliability of the solution, and device usage and performance, in accordance with the TO.
9. MDM Security/Compliance Reports – Security reports include all data relevant to the monitoring and support of the system's vulnerabilities and defenses, including attempts at fraud in accordance with the TO. Security status reports shall be run as requested.
10. The following capabilities may be defined at the TO level:
    a) (Optional) Quality of Service (QoS) – shall support QoS capabilities to prioritize real-time or latency-sensitive application data where appropriate (e.g.: VoIP, video, real-time chat). It shall be possible to enforce and exclude QoS priority by application or protocol to prevent non-real-time applications from inappropriately increasing their traffic priority.
    b) (Optional) Classified Data – shall support access classified data up to the SECRET level via mobile devices.
    c) (Optional) PIV/CAC Support – shall support the management of PIV/CAC cards on mobile devices via the MDM.
    d) (Optional) Biometric Support – shall support biometric support such as fingerprint or face recognition with mobile devices. The ability for the MDM to manage this capability may be combined with PIV / CAC support.
    e) (Optional) Network Monitoring – shall support monitoring of the mobile device network quality and performance (e.g., the number and location of dropped calls by enterprise/agency devices).

C.2.8.6.1.4.2 Mobile Application Management (MAM)

The following capabilities are mandatory unless marked optional:

1. Application Deployment:
    a) Commercial Application Store (enable/disable)
    b) Reporting of installed applications
    c) Block application purchase

d) Application Whitelisting/Blacklisting
e) Staged/controlled application deployment (limit deployment by policy, group, location, etc. to facilitate gradual deployment of new or updated applications)

2. Mobile Application Store (MAS):
   a) MAS shall allow users to select private enterprise/agency applications for installation on managed devices. This capability shall be integrated into the MDM portal and shall allow application provisioning by group policy and mandatory application deployment. MAS shall support the following capabilities:
      i. Add/update an application from a Commercial Application Store to the MAS
      ii. Add/update an enterprise/agency application to the MAS via a web GUI
      iii. Add additional metadata to and report on metadata on any application added to the MAS (name, description, version, OS, keywords, etc.)
      iv. Specify the effective date for an agency internal application
      v. Specify the expiration date for an agency internal application
      vi. Specify the minimum operating system and model for an agency internal application
      vii. Download agency internal and public applications from MAS
      viii. Categorize, group or tag applications (e.g., business applications, scientific applications, etc.)
3. Application Security:
   a) Mutual Authentication – MDM applications on the device and services must mutually authenticate using certificate-based authentication to ensure the communications channel is not intercepted.
   b) Application Installation Control – shall support relevant authorizations and approvals (include change tracking) to control downloading of authorized and unauthorized applications and help ensure user compliance. This includes the ability to monitor application usage.
   c) Blacklisting / Whitelisting –block and/or remove specified applications (Blacklisting), and permit or force the installation of specified applications (Whitelisting).
   d) Application Environment Requirements – detect and enforce device environment conditions such as:
      i. Minimum or specific operating system versions
      ii. Required presence or absence of other applications

iii. Absence of privilege escalation (“rooting” or “jailbreaking”)

e) Application Signing – shall support requiring digital signatures for application installation, from both commercial and private application stores and direct application push / deployment.

4. The following capabilities may be defined at the TO level:
   a) (Optional) Third-party Application Mutual Authentication to provide third-party applications with mutual authentication and secure communications through wrappers, binary patching, etc.
   b) (Optional) MAM Software Integration Services to support the delivery of new or existing enterprise/agency applications to mobile devices, such as data entry system accessible to field workers.

C.2.8.6.1.4.3 Mobile Content Management

MCM enables secure mobile access to content anytime, anywhere, and on any device. It protects sensitive content and provides users with a central application to securely access, store, update and distribute documents.

C.2.8.6.1.4.4 Mobile Security

The following capabilities are mandatory unless marked optional:

1. Enroll a device before applying any policy (null policy)
2. Create Whitelists/Blacklists for device enrollment to include OS versions and device models
3. Allow enrollment of untrusted devices and anonymous / unknown users outside the enterprise as individuals or to groups under the MDM
4. Use an existing MDM user attribute repository for enrollment to the new MDM system
5. Take action based on compliance rules, in support of MDM’s ability with active (device scanning) and passive (on-access scanning) tools to detect, report, and alert on a compromised device (e.g.: jail broken / rooted device, malware)
6. Block the device or to erase (wipe) only the managed data on a device under the following conditions:
   a) Blacklisted operating system or version (policy based)
   b) Exceeding a set number of failed access attempts to the device or MDM application (policy based)
   c) Exceeding defined interval for contacting MDM (policy based)
   d) Detection of OS jailbreaking or application tampering (policy based)
   e) Any other policy violation

f) Remote instruction from MDM (manual)

7. Password policy enforcement:
   a) Minimum complexity (length, composition, common words, etc.)
   b) Password lifetime limit
   c) Password re-use limits
   d) Password inactivity timeout (grace period) for device and MDM application
   e) Report password failures beyond threshold to MDM
   f) Maximum password attempts before lock or wipe
8. Mask passwords when they appear in the Management GUI
9. Determine which administrative user made a configuration change in the MDM administrative environment
10. Determine which device user made a configuration change in the MDM console (self-service logging)
11. Installation and configuration (update, revocation checking, revocation) of individual and group soft authentication certificates for the following purposes:
    a) Email (S/MIME) signing and encryption
    b) Wi-Fi Configuration
    c) VPN Configuration
12. Send/receive (encrypt and sign, decrypt and verify) messages that use PKI or S/MIME encryption, where email functionality is delivered by the service/system
13. Restrict downloading attachments, copying of data to/from removable media, or otherwise create separate spaces or virtual containers for agency data and applications from personal data
14. (Optional) View the current GPS location of a device or logical grouping of devices on a map
15. Encrypt the data in transit between the MDM and the device in accordance with FIPS 140-2
16. The data at rest on a mobile device shall be separated in different containers for agency data and personal data, and shall protect agency data from access by uncontrolled applications to limit interaction between agency data and personal data. The agency data shall be encrypted if the underlying platform does not encrypt all data on the device.
17. User Authentication shall support PIN or password authentication for the managed applications, and optionally multifactor authentication with any two of the following three authentication types:
    a) Shared Secret – something the user knows, like a PIN or password

b) Token – something a user possesses such as a cryptographic key such as an RSA token (soft or hard), a challenge/response token, a PIV or CAC, or a key generator device
c) Biometric – a sufficiently unique physical characteristic of the user, such as a fingerprint, iris or facial image

18. User Compliance:
    a) Set up compliance rules to include custom compliance rules for profiles, devices, groups, and Whitelist/Blacklist
    b) Activate/deactivate a compliance rule
    c) Specify user and group rules for application compliance, such as required or prohibited applications on a device
    d) Provide enterprise level compliance reports, including lost/wiped/inactive devices, the total number of devices, the number of devices active, how much data is sent/received by devices, and connection type
19. Alerting – notify agency operations staff about agency devices:
    a) Set up custom alerts to users and management based upon various parameters
    b) Send custom alerts to one or more user roles including administrators
    c) Specify a creation policy for custom alerts to include having various alert severity levels
    d) Create automated alerts for security issues such as compromised devices
    e) Create alerts based upon device status such as battery low, device roaming, equipment down (not responding), device inactive, etc.
    f) View alerts pending acknowledgement
    g) Acknowledge alerts and track acknowledgements
20. Audit reports – provide data necessary to monitor, reconcile, and audit system processing and reconciliation activities. Audit reports shall be exportable, and shall be run as requested by the agency.
    a) Administrator activity (actions performed, time stamps, etc.)
    b) User access times and enrollments
    c) Devices (number of devices by agency and across all sub-agencies, type, OS version, etc.)
    d) Console logins and functions (connections to the management console, actions performed, etc.)
    e) Policy changes and versions (policy revision control and historical changes)
    f) Policy violations

21. Safeguard any Personally Identifiable Information (PII), including directory data stored in the information system in accordance with NIST SP 800-122.

C.2.8.6.1.4.5 Deployment Support

The following capabilities are mandatory unless marked optional:

1. Deployment:
   a) The contractor shall support MMS for installing, configuring, and certifying the initial deployment of the MDM, MAM and Container solutions, as well as the ability to support specific agency- related integrations or customizations, as specified in the TO. The contractor shall assist the agency with achieving accreditation and authorization (compliance) objectives by producing supporting documentation and/or modifications to the solution to reach compliance.
2. Enterprise Systems Integration:
   a) The contractor shall assist in deploying and integrating its MMS into the agency-wide environment. This includes systems such as enterprise email, directories, trouble-ticketing, etc.
3. Training:
   a) The contractor shall provide MDM/MAM training material content, as well as providing pre-packaged online training and associated materials in accordance with the TO.
4. Help Desk:
   a) The contractor shall provide a Help Desk for MDM/MAM that supports online requests / resolutions via email and telephone.

C.2.8.6.2 Features

None.

C.2.8.6.3 Interfaces

The MMS shall support the UNIs for all Smartphones and Tablets (based on smartphone OSs) operating under 3G/4G Cellular Service (based on standards for CDMA, GSM, and LTE) as required.

C.2.8.6.4 Performance Metrics

The MMS performance levels and AQL of KPIs in Section C.2.8.6.4.1 are mandatory unless marked optional.

C.2.8.6.4.1 Managed Mobility Service Performance Metrics

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Event Notification (EN)	Routine	Next business day or within 24 hours for a Low category event	≤ Next business day or 24 hours	See Note 1
		Within 4 hours of a Medium category event	≤ 4 hours	
		Within 30 minutes of a High category event	≤ 30 minutes	
Grade of Service (Configuration Change)	Routine	Within 5 hours for a Normal priority change	≤ 5 hours	See Note 2
		Within 2 hours for an Urgent priority change	≤ 2 hours	
Telephone Incident Response Time	Routine	Within 1 hour of the notification for a Low category incident	≤ 1 hour	See Note 3
		Within 15 minutes of the notification for a High category incident	≤ 15 minutes	
Dispatch Incident Response Time	Routine	Within 36 hours of the notification for a Low category incident	≤ 36 hours	See Note 4
		Within 24 hours of the notification for a High category incident	≤ 24 hours	

Notes:

1. The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification of the agency. Events are categorized as follows:

   a) Low — Events in the Low category have a negligible impact on service. They include firewall incidents that do not significantly affect network security, as well as minor hardware, software and configuration problems.

b) Medium — Events in the Medium category have a more serious impact on service, and may indicate a possible security breach, threat or attack attempt. They may also cause the service to operate in a degraded state.

c) High — Events in the High category represent firewall violations that severely impact service and operations. They indicate a true compromise of network security. These events also include major hardware, software and configuration problems, and are immediately reported via email or telephone, as specified by the agency.

2. The Grade of Service (Configuration Change) value represents the elapsed time between the configuration change request and the change completion. Changes are initiated and prioritized by the agency, or may be implemented in response to an event. Changes initiated by the contractor require agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency).
3. The Telephone Incident Response value represents the elapsed time between the agency's notification to the contractor, and the contractor's implementation of response procedures. These procedures, as well as what constitutes Low and High incidents, are defined in the TO.
4. The Dispatch Incident Response value represents the elapsed time between the agency's notification to the contractor, and the contractor's arrival to the affected site for implementation of response and investigative procedures. These procedures, as well as what constitutes Low and High incidents, are defined in the TO.

C.2.8.7 Audio Conferencing Service

C.2.8.7.1 Service Description

The government has a large community of audio conferencing users. The following sections provide the requirements for Audio Conferencing Service (ACS).

C.2.8.7.1.1 Functional Definition

ACS enables participants to engage in a multi-point audio conference call. The audio connection from the conference participants to the ACS conference-bridge is provided by voice service (IPVS, CSVS) and cellular voice service.

C.2.8.7.1.2 Standards

ACS shall comply with the following standards:

1. ANSI T1.101 for T1
2. ANSI T1.607 and 610 for ISDN

3. ANSI SS7, and enhanced SS7 standards for interworking (e.g., address translation) between circuit-switched network and IP network
4. Telcordia Notes on the Networks (SR-TSV-2275)
5. IETF RFC 3661 through 3665 for SIP (Session Initiation Protocol)
6. IETF RFC 3435 for MGCP (Media Control Gateway Protocol)
7. ITU-TSS H.323/225/245/248 (enhanced for VoIP)

The contractor shall comply with new versions, amendments, and modifications made to the standards listed above.

C.2.8.7.1.3 Connectivity

ACS shall connect to and interoperate with:

1. Customer-specified locations
2. PSTN
3. Internet
4. The contractor's network and all other contractors' networks for CSVS and IPVS

C.2.8.7.1.4 Technical Capabilities

The following ACS capabilities are mandatory unless marked optional:

1. Multi-point Bridging Capability. Support selective two-way or one-way conversations between conferencing ports (i.e., allow a subset of conferees to participate in a two-way conference while the remaining conferees are listeners only). During a multi-point conference, the addition of a party to, or the deletion of a party from, the conference shall be indicated by a tone or verbal announcement.
2. Conference Set-up Capability. Provide the following conference set-up support services:
    a) User-Controlled Conference. Allow authorized users and users with a calling-card to establish a conference call by dialing a designated number to access the service. The following two automated modes of user-initiated conferencing capabilities shall be supported:
        i. Meet-Me Conference – Allow each user to be connected in a conference by dialing a designated number and authorization/pass code at a predetermined time or as directed by the operator. For recurring meet-me conferences, the contractor shall permit the participants to reuse the same dial access number and authorization/pass code and allow bookings of recurring conferences.
        ii. Preset Conference – Allow an authorized user to activate a previously-defined conference with associated conferees by dialing an access

number followed by an authorization/pass code. Once activated, the system shall attempt to connect the pre-designated participants using the predefined lists.

b) Attendant-Assisted Conference. Allow operators to establish a conference. Conferees shall be able to call an operator during a conference for immediate attention, such as general assistance or adding or dropping participants.

3. Audio Conference Reservation System.
4. Automatic port expansion. Support, without operator assistance, automatic expansion to support additional users to the conference in progress beyond the dial-in ports reserved as long as facilities are available.
5. Conferee tones. Enable or disable conferee tone when a participant enters or exit a conference.
6. Participant count.
7. Roll call.
8. Attendant assistance. Available at any time during an audio conference.

C.2.8.7.2 Features

The following ACS features are mandatory unless marked optional.

1. Audio recording of call. Allow recording of conference call into storage media for later replay.
2. Spanish language translation. Provide language translation to English from Spanish for transcription of a pre-recorded audio conference.
3. (Optional) Language translation. Provide language translation to English from languages other than Spanish for transcription of a pre-recorded audio conference.
4. Moderator-led Q&A.
5. Participant list report.
6. Password-protected session.
7. Download and replay a pre-recorded audio conference.
8. Transcription of audio call.
9. Temporary blocking. Allow temporary blocking of audio conference participants in order to remove a sub-set of participants/users from the conference.

10. (Optional) Secured Audio Conference. Support sensitive voice conferences with end-user encryption for discussions of a CUI nature between multiple locations with protection from unauthorized interception (i.e., eavesdropping).
11. Operator dial-out. The capability to add a participant to a conference via an outbound call from the conference bridge initiated by the conference attendant.
12. Host dial-out. The capability to add a participant to a conference via an outbound call from the conference bridge initiated by the conference host.
13. Executive conference. Conference requires professional moderator assistance with control of conference attendant functions.
14. International global meet. The feature provides in-country local access which is a non-North American toll number assigned to a specific country and bridge.
15. Host controls. The conference host has the capability to control conference attendant functions.

C.2.8.7.3 Interfaces

The contractor shall support audio connection to the conference bridge from services such as voice service (e.g., CSVS and IPVS), and cellular voice service.

C.2.8.7.4 Performance Metrics

The ACS performance levels and AQL of KPIs are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
GOS (Operator Assistance Response Delay)	Routine	30 seconds	≤ 30 seconds	See Note 2
Time to Restore	With Dispatch	8 hours	≤ 8 hours	
	Without Dispatch	4 hours	≤ 4 hours	

Notes:

1. ACS availability is calculated as a percentage of the total reporting interval time that ACS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. GOS (Operator Assistance Response Delay) is the delay experienced by conference participants to receive operator assistance during a conference. Delay is measured as the interval between the end of signaling (e.g., dialing for operator assistance) and the receipt of voice response from the operator.

C.2.8.8 Video Teleconferencing Service

C.2.8.8.1 Service Description

Video Teleconferencing Service (VTS) enables participants at different locations to simulate face-to-face meetings and conduct interactive dialogue with instant sharing of various applications and documents.

C.2.8.8.1.1 Functional Definition

VTS will offer point-to-point and multi-point conferencing with audio conference add-on capabilities to support the following three user configurations: 1) desktop, 2) portable roll about, and 3) fixed conference room locations.

C.2.8.8.1.2 Standards

VTS shall comply with the following standards:

1. Federal Telecommunications Recommendations (FTR) 1080B - 2002 (hereinafter referred to as FTR-1080) issued by the Technology and Standards Division of the National Communication System (NCS).
2. FTR 1080 encompasses the specifications for narrow-band audio and video teleconferencing, from 56 Kbps to 1920 Kbps, primarily based on the following standards:
   a) ITU-T H.320 recommendations for telephony networks
   b) ITU-T H.323 recommendations for packet based multi-media conferencing
   c) ITU-T H.239 for H.320 for document conferencing
3. IETF RFC 3261 Session Initiation Protocol (SIP).

The contractor shall comply with new versions, amendments, and modifications made to the documents and standards listed above.

C.2.8.8.1.3 Connectivity

VTS shall connect to and interoperate with:

1. IP Networks
2. PSTN

C.2.8.8.1.4 Technical Capabilities

The following VTS capabilities are mandatory unless marked optional:

1. Allow participants at different physical locations to simulate in-person meetings and conduct interactive dialogue using point-to-point and point-to-multi-point video teleconferencing arrangements.
2. Support two-way video, one-way video with interactive voice, and/or the instant sharing of various types of documents/data files among VTS participants as an adjunct to the video teleconferencing session.
3. Support document sharing (data conferencing) which enables conference participants to interactively view, edit, and share or transfer data files and documents.
4. Provide an audio conference add-on capability to support non-video conference participants in a VTS call.
5. Provide teleconferencing bridge capabilities.
6. Support the following modes of operation:
    a) Dial-Out mode: A centralized arrangement where the conference bridge operator initiates a call and dials each participant
    b) Meet Me (Dial-In) mode: Each participant is responsible for individually initiating a call and dialing into the conference bridge.
    c) Mixed Dial mode: Support a combination of both dial-out and meet me (dial-in) callers
7. Provide the capability for VTS users to request operator assistance to resolve technical issues.
8. Maintain synchronization between the audio and video signals.
9. Allow users to establish a point-to-point VTS on demand without a reservation. Point-to-point VTS shall include full-duplex video, audio, and ancillary data transmission between participating locations.
10. Provide VTS multi-point arrangements in conjunction with the contractor's VTS reservation system. The multi-point arrangement shall have the capability of simultaneously providing VTS to users of a different EIS contractor's network and to users of public or other private networks. During a multi-point conference, the

addition of a party to, or the deletion of a party from, the conference shall be indicated by a tone or by a verbal or visual announcement.

11. Provide access to a secure central reservation system to permit authorized VTS users to schedule multi-point video teleconferences.
12. Provide a video format conversion capability that permits operation between the following:
    a) CODECs which operate in the NTSC video format and CODECs which operate in the Phase Alternation by Line (PAL) video format.
    b) CODECs which operate in the NTSC video format and CODECs which operate in the Système Electronique Couleur Avec Memoire (SECAM) video format.
13. Traverse and successfully interoperate with agency firewalls and security layers. The contractor shall verify with the agency that the agency firewall is compatible with this service.
14. Provide VTS reports in accordance with the TO.

C.2.8.8.2 Features

The following VTS features are mandatory unless marked optional:

1. Attended Service: The contractor shall provide call monitoring, roll call, and coordination for a VTS conference.
2. Verification: The contractor shall provide pre-testing, registration, and verification that agency-owned equipment operates correctly with the contractor's VTS.
3. Coding Conversion (Transcoding):
    a) Provide transcoding that is compliant with FTR 1080 formats.
    b) (Optional) Provide a coding conversion capability that permits operation between CODECs, all of which use the National Television Standards Committee (NTSC) video format, but none of which support the FTR 1080 standard and none of which use the same encoding/decoding algorithm(s). At a minimum, the contractor shall support the following compression algorithms as needed by the agency: SG3/SG4, CTX, and CTX+.
    c) (Optional) Provide a coding conversion capability that permits operation between CODECs, all of which use the NTSC video format, in which one or more of the CODECs support the FTR 1080 and in which one or more of the CODECs do not support the FTR 1080. At a minimum, the contractor shall support the following compression algorithms as needed by the agency: SG3/SG4, CTX, and CTX+.

4. (Optional) Rate Adaptation: Provide a data rate adaptation capability to ensure that all VTS locations participating in a video teleconference can interconnect with each other at dissimilar data rates.
5. (Optional) Security – CUI: Provide transparent and secure VTS communications paths to support CUI video communications. The security capabilities are described in the FTR1080 recommendation.
6. (Optional) Security – Classified: Provide transparent and secure VTS communications paths and support video information that is categorized as classified (National Security agency type 1 encryption) video communications. The security capabilities are described in the FTR1080 recommendation.

C.2.8.8.3 Interfaces

The VTS UNIs at the SDP as defined in Section C.2.8.8.3.1 are mandatory unless marked optional.

C.2.8.8.3.1 Video Teleconferencing Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Digital Trunk: T1 (Std: Telcordia SR-TSV-002275 and ANSI T1.102/107/403)	Up to 1.536 Mbps	T1 Robbed-Bit Signaling
2	Digital Trunk: ISDN PRI T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
3 (Non-Domestic / OCONUS)	Digital Trunk: E-1 Channelized (Std: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
4	All IEEE 802.3 cable and connector types	Up to 100 Mbps	IEEE 802.3. IPv4 and IPv6

1. If the agency provides the CODEC and the inverse multiplexer, and the contractor provides only reservation, coding conversion, and/or format conversion, the UNIs supported shall include:
   a) ITU-TSS V.35

b) EIA RS-449
c) EIA RS-530
d) RJ-x (e.g., RJ-45)
e) Data Interface(s) – the VTS shall support any combination of the following:
   i. EIA RS-232
   ii. EIA RS 449
   iii. ITU-TSS V.35
   iv. EIA RS-530

C.2.8.8.4 Performance Metrics

The VTS performance levels and AQL of KPIs in Section C.2.8.8.4.1 are mandatory unless marked optional.

C.2.8.8.4.1 Video Teleconferencing Service Performance Metrics

KPI	User Type	Performance Standard (Threshold)	AQL	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Grade of Service (Completed Service Requests)	Routine	95% of VTS conference requests met	≥ 95%	See Note 2
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Availability is measured and calculated as a percentage of the total reporting interval time that VTS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. The Grade of Service (completed service requests) applies to video conferences that are reserved and confirmed. It shall be calculated as the ratio of the number of locations successfully completing a VTS call divided by the total number of locations scheduling a VTS call within a calendar month. Locations that schedule a video conference and then decide not to join will be treated as successfully completing a VTS call for Grade of Service (Completed Service Requests). The contractor shall compute the number of completed service requests by counting the cumulative number of locations associated with each conference that were successfully completed. The contractor shall compute the number of service requests denied by counting the cumulative number of locations associated with each VTS conference that could not be scheduled for a particular date and time requested in a calendar month. VTS calls that were disconnected and then re-established only due to the fault of the contractor would be included as a denied request.

C.2.8.9 DHS Intrusion Prevention Security Service (DHS Only)

The Intrusion Prevention Security Service (IPSS) consists of the use of classified and unclassified Government Furnished Information (GFI) within software, hardware, and service components that monitor, identify and mitigate potential cyber security threats. The service monitors Internet traffic bound for or originating from the federal government, detects signs of malicious cyber activity, and prevents that traffic from jeopardizing the confidentiality, integrity, availability, and control of Participating Agency networks (i.e., agencies who enter into a Memorandum of Agreement with the Department of Homeland Security (DHS) to authorize the application of intrusion prevention capabilities by DHS and DHS contractors to approved agency traffic).

C.2.8.9.1 Service Description

C.2.8.9.1.1 Functional Definition

This service includes the following set of functions:

1. Indicator management
2. Detection
3. Response and Protection
4. Alerting and Reporting

Indicator management covers work necessary to manage and share cyber threat indicators and countermeasures. Detection covers access to network traffic and the application of a wide range of capabilities to inspect that traffic and identify malicious activity. Response and Protection functions cover capabilities that apply

countermeasures to prevent and manage malicious activities. Alerting and reporting covers event notification and forensic artifact handling.

C.2.8.9.1.2 Standards

This service shall comply with the following standards and guidance:

- ICD 703 – Protection of Classified National Intelligence, Including Sensitive Compartmented Information
- NSA Security Guidelines for IPSS/ECS
- CNSSI 1253 – Security Categorization and Control Selection for National Security Systems, 27 March 2014
- NIST SP800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations
- US-CERT Standard Operating Procedures (SOPs) SOP 108 – Identifying Sensitive Information: PII Handling and Minimization, and SOP 110 - PII Handling & Minimization

The contractor may propose alternatives at no additional cost to the government that meet or exceed required technical capabilities; DHS Network Security Deployment security representatives should be consulted.

C.2.8.9.1.3 Connectivity

DHS IPSS shall connect with EINSTEIN Enclaves, examine Participating Agency traffic meeting the definition of “External Traffic” in TIC v2.0 and as described in Section C.1.8.8 paragraph 3, and connect to the DHS US-CERT data centers.

C.2.8.9.1.4 Technical Capabilities

The DHS IPSS requires the following minimum, mandatory capabilities.

1. Establish and support a process that allows DHS to provide cyber threat indicators and define desired effects in the protection of covered network traffic.
2. Demonstrate to DHS that IPSS operates as intended when traffic is present that matches malicious indicators prior to the activation of new or modified indicators and their associated actions.
3. Support a process that allows DHS to direct actions on network traffic to gather additional information on cyber threats, stop cyber attacks, and/or respond to cyber incidents.
4. Provide for the ability to receive, accept, utilize, and secure GFI up to the Top Secret/Sensitive Compartmented Information (TS/SCI) level, including PII, such

as cyber threat indicators signatures, and associated actions in accordance with DHS-approved security guidelines.

5. Provide an automated means for DHS to share GFI and utilize the GFI provided within the DHS IPSS in as near real-time as possible.
6. Establish or leverage additional commercially available cyber threat information and/or DHS IPSS functional capabilities to provide additional protections for Federal Systems.
7. Ensure only those indicators and associated actions that are approved and further specified by DHS are applied to Participating Agencies.
8. Provide the ability to apply different sets of mitigation capabilities to a Participating Agency's traffic that does not affect which mitigations are applied to a separate Participating Agency's traffic.
9. Ensure that GFI is not disclosed or shared with any third party or used for any purpose that DHS has not specifically authorized.
10. Gain access to approved Participating Agency Federal System network traffic that uses the contractor as its Internet service provider.
11. Establish the ability to detect malicious network traffic to support the DHS IPSS and to provide additional contextual information associated with alerts to support post-incident analysis
12. Support signature-based, heuristic-based and/or other emerging detection methods.
13. Provide solutions that allow for the detection of malicious activity within encrypted traffic.
14. Support a wide-range of unclassified and/or classified protection measures. The kinds of protection measures the government expects to be available via a DHS IPSS can best be described by referencing the NIST Guide to Intrusion Detection and Prevention Systems. The guide defines typical IPSS capabilities as providing the capability to:
    - collect more detailed information for a specific session after malicious activity has been detected
    - prevent or block a detected threat by terminating the network connection or blocking access to the target
    - change the attack's content by removing or replacing malicious portions of an attack to make it inoperable
    - see evasion techniques and duplicate processing performed by a target

- tune detection accuracy so that an organization can achieve an optimum mix of false positives to false negatives in line with that organization's risk tolerance

15. Include the ability to redirect to a safe server.
16. Allow for the capturing and storing of analytically relevant data associated with potential harmful network traffic specific to some indicators but and not necessarily applied to all indicators.
17. Ensure that the DHS IPSS technology does not retain traffic other than traffic associated with suspected malicious activity or as otherwise required by DHS.
18. Apply DHS-directed prevention services, as defined and approved by the United States Computer Emergency Readiness Team (US-CERT).
19. Apply DHS-directed prevention services through an approved traffic segregation solution to only designated, Federal System network traffic.
20. Operate as an in-line service (i.e., a service within the ISP network boundary that is capable of performing mitigation actions as traffic traverses the ISP network in the normal flow of traffic) that detects and mitigates malicious IP-based traffic. For the purposes of this contract and to maximize contractor flexibility, the term "in line" should not be construed as mandating a specific network architecture, rather, the service should ensure that the following two conditions are met:
    a) All Internet traffic delivered to the Participating Agency's SDP shall be monitored and subject to mitigation by the Prevention Service prior to said delivery.
    b) All Participating Agency traffic delivered to the Internet via the Participating Agency's SDP shall be monitored and subject to mitigation by the Prevention Service prior to said delivery.
21. Define and apply the full range of existing and future DHS IPSS functional capabilities (typically defined in a technology roadmap) at cyber-relevant speed to counter cyber threats and attacks.
22. Provide quarantined malware to Participating Agency and to DHS via the US-CERT malware lab or other specified DHS entity.
23. Prior to utilization of cyber threat indicators, signatures, and/or countermeasures, demonstrate to the government that cyber threat indicators, signatures, and/or countermeasures provided operate as intended.
24. Provide DHS and Participating Agencies with detection alerts and associated contextual information around suspicious traffic sufficient to identify the facts of a

particular incident or attempted incident for protected traffic in accordance with DHS specifications or guidance.

25. Provide DHS and Participating Agencies with data to support network traffic pattern assessments to detect and address anomalous patterns that may be indicators of malicious activity in accordance with DHS specifications or guidance.
26. Provide DHS and Participating Agencies with information related to indicators, signatures, associated actions, and/or alerts over a given time period.
27. Ensure that agency network traffic and other information are not disclosed to any party other than DHS and the agency and then only as specifically identified under this contract and task orders thereto, and take necessary steps to ensure Participating Agency data is secure from unauthorized access, use, disclosure, or retention.
28. Provide test results and support a process that allows for government participation and observation in tests.
29. Within 15 minutes of discovery, notify DHS of any unauthorized access, use, disclosure, or retention of Participating Agency data, and of any breach of any security or information handling requirements or additional instructions provided by DHS regarding the handling of Participating Agency network traffic, and provide relevant information to allow DHS to assess the scope of any such breach.
30. Provide an ICD 705 Sensitive Compartmented Information Facility (SCIF) and personnel with TOP SECRET/SCI clearances. Facility size, number of personnel and other details to be provided with DHS Task Orders.

C.2.8.9.2 Features

The following features are mandatory:

1. Classified Email Threat Detection and Countermeasures. The contractor shall provide capabilities that apply sensitive and classified (up to TS/SCI) indicators and countermeasures offered by DOD/DHS to email messages and with real-time secure exchange with DHS for global awareness.
2. Classified DNS Threat Detection and Countermeasures. The contractor shall provide capabilities that apply sensitive and classified (up to TS/SCI) indicators and countermeasures offered by DOD/DHS to DNS queries and responses and with real-time secure exchange with DHS for global awareness.

3. Additional countermeasures as specified by DHS.

C.2.8.9.3 Interfaces

The contractor shall support the UNI at the SDP to connect to the DHS IPSS as Ethernet Access defined in Section C.2.1.2.

C.2.8.9.4 Performance Metrics

Performance metrics for this service shall be defined in the TO.

C.2.9 Access Arrangements

C.2.9.1 Access Arrangement Description

Access Arrangements (AAs) connect the SDP at the agency location to a POP on the contractor's network. The range of line speeds and reliability options allows agency users to satisfy their diverse needs to access contractor networks. AAs provide the convention to specify and price the originating and/or terminating access component required to deliver a service. AAs cannot be ordered as a standalone access service and no performance metrics are specified for them.

C.2.9.1.1 Functional Definition

AAs can be used for any application such as voice, data, video, and multimedia. AAs shall provide diversity options that include, but are not limited to:

1. Physically disparate, diverse paths from the SDP to the POPs of two diverse contractors.
2. Physically disparate, diverse paths from the SDP to the contractor's POP.
3. Redundant paths from an SDP to the contractor's POP.

Special construction may involve providing a special service or facility related to the delivery and/or performance of a service requirement. This shall include the following situations:

1. An access arrangement does not exist or does not have sufficient capacity, and the contractor has to provide special construction through the implementation, rearrangement or relocation of physical plant solely for the government-requested access arrangement.
2. The contractor uses special construction to implement a different route (government premises to a PCL, PCL to an alternate contractor's POP, or some other type of route) than that which the contractor would otherwise use to provide an access arrangement for the government.

When necessary to fulfill an order, the contractor shall perform site surveys of potential operational locations to collect and validate floor plans, physical measurements, building power capacity, and external ingress/egress factors. The contractor shall deliver site survey reports after the completion of the physical site visits. See Section J.10 for the special access construction template for the site survey report.

C.2.9.1.2 Standards

AAs shall comply with the following standards:

1. ANSI T1.102/107/403/503/510 for T1
2. ANSI T1.607/610 for ISDN PRI
3. Telcordia PUB GR-499-CORE for T3
4. ANSI T1.105 and 106 for SONET
5. Telcordia PUB GR-253-CORE for SONET
6. ITU-TSS G.702 and related recommendations for E1 and E3
7. Frequencies grid and physical layer parameters for Optical Wavelength:
   a) DWDM: ITU G.692 and G.694 as mandatory and G.709 and G.872 as optional
   b) WDM: ITUG.694.2 and Telcordia GR 253
8. Applicable Telcordia for DWDM systems are GR-1073, GR-1312, GR-2918, GR-2979 and GR-3009
9. EIA/TIA-559, Single Mode Fiber Optic System Transmission Design
10. Telcordia GR-20-CORE for Generic Requirements for Optical Fiber and Optical Fiber Cable GR-253 (SONET), and GR-326 (Connector)
11. Digital Subscriber Line (DSL) - ADSL and SDSL:
    a) ADSL and DSL Forums
    b) ITU-TSS Recommendation G.992 for ADSL (interoperable DSL modem and DSLAM line card)
    c) ANSI T1.413 (compatible DSL modem and DSLAM line card from the same manufacturer)
12. ISDN based DSL (IDSL): ISDN Forums
13. Ethernet Access: IEEE 802.3, including 10 Base-T/TX/FX, 100 Base-TX/FX, 1000 Base-T/FX/L/LX/B/BX/PX, and 10/40/100 Gigabit Ethernet (IEEE 802.3ae and 802.3ba)

14. Cable High-Speed Service: DOCSIS (Cable Labs) standards
15. The contractor shall comply with all new versions, amendments, and modifications to the above documents and standards

C.2.9.1.3 Connectivity

AAs shall connect to and interoperate with:

1. Agency-specified locations and equipment
2. Contractor's network POPs

C.2.9.1.4 Technical Capabilities

The following AA capabilities are mandatory unless marked optional:

1. Integrated access of different services
2. Transparent to any protocol

The following AAs are mandatory unless marked optional:

1. **T1**. A line rate of 1.544 Mbps, which may be used to provide channelized or unchannelized T1 access arrangement as follows:
   a) Channelized T1. In this mode, 24 separate DS0s clear channels of 56/64 kb/s shall be supported.
   b) Unchannelized T1. In this mode, a single 1.536 Mbps information payload shall be supported.
2. **ISDN PRI**. This category of AA shall support 23 separate DS0 clear channels of 56/64 kbps over an interface of ISDN PRI (23B+D) with a line rate of 1.544 Mbps.
3. **ISDN BRI**. This category of AA shall support 2 separate DS0 clear channels of 56/64 kbps over an interface of ISDN BRI (2B+D) with a line rate of 144 Kbps.
4. **T3**. This category of AA shall support a line rate of 44.736 Mbps, which may be used to provide channelized or unchannelized T3 access arrangement as follows:
   a) Channelized T3. In this mode, 28 separate DS1 channels of 1.536 Mbps information payload rate shall be supported.
   b) Unchannelized T3. In this mode, a single 43.008 Mbps payload shall be supported.
5. **E1** This category of AA shall support a line rate of 2.048 Mbps, which may be used to provide channelized or unchannelized E1 service as follows:

a) Channelized E1. In this mode, 30 separate DS0 clear channels shall be supported.
b) Unchannelized E1. In this mode, a single 1.92 Mbps information payload shall be supported.

6. **E3** This category of AA shall support a line rate of 34.368 Mbps, which may be used to provide channelized or unchannelized E3 service as follows:
   a) Channelized E3. In this mode, 16 separate E1 channels shall be supported.
   b) Unchannelized E3. In this mode, a single 30.72 Mbps information payload shall be supported.
7. **SONET OC-3. T**his category of AA shall support a line rate of 155.520 Mbps, which may be used to provide channelized OC-3 or concatenated OC-3c access arrangement as follows:
   a) Channelized OC-3. In this mode, three separate OC-1 channels, each with an information payload data rate of 49.536 Mbps, shall be supported.
   b) Concatenated OC-3c. In this mode, a single channel equivalent to information payload data rate of 148.608 Mbps shall be supported.
8. **SONET OC-12**. This category of AA shall support a line rate of 622.080 Mbps, which may be used to provide channelized OC-12 or concatenated OC-12c access arrangement as follows.
   a) Channelized OC-12. In this mode, 4 separate OC-3 channels, each with an information payload data rate of 148.608 Mbps, shall be supported.
   b) Concatenated OC-12c. In this mode, a single channel equivalent to an information payload data rate of 594.432 Mbps shall be supported.
9. **SONET OC-48**. This category of AA shall support a line rate of 2.488 Gbps, which may be used to provide channelized OC-48 or concatenated OC-48c service as follows:
   a) Channelized OC-48. In this mode, 4 separate OC-12 channels, each with an information payload data rate of 594.432 Mbps, shall be supported.
   b) Concatenated OC-48c. In this mode, a single channel equivalent to an information payload data rate of 2.377728 Gbps shall be supported.
10. **SONET OC-192**. This category of AA shall support a line rate of 10 Gbps, which may be used to provide channelized OC-192 or concatenated OC-192c service as follows:
    a) Channelized OC-192. In this mode, 4 separate OC-48 channels, each with an information payload data rate of 2.488 Gbps, shall be supported.

b) Concatenated OC-192c. In this mode, a single channel equivalent to an information payload data rate of 9.510912 Gbps shall be supported.

11. **(Optional) SONET 768**. This category of AA shall support a line rate of 40 Gbps, which may be used to provide channelized OC-768 or concatenated OC-768c service as follows:
    a) Channelized OC-768. In this mode, 4 separate OC-192 channels, each with an information payload data rate of 9.510912 Gbps, shall be supported.
    b) Concatenated OC-768c. In this mode, a single channel equivalent to an information payload data rate of 38.486016 Gbps shall be supported.
12. (Mandatory if CSVS or PLS analog transport is offered, optional otherwise) **Analog Line (4 KHz)**. This category of AA shall support 2 wire analog lines and trunks without access integration for voice service.
13. **DS0**. This category of AA shall support information payload data rates of 56 kbps and 64 kbps.
14. **(Optional) Subrate DS0**. This category of AA shall support Subrate DS0 at information payload data rates of 4.8, 9.6, and 19.2 kbps.
15. **Optical Wavelength**. Bi-directional wavelengths (WDM) connections to an optical network for the following speeds:
    a) 1 Gbps.
    b) 2.5 Gbps.
    c) 10 Gbps.
    d) 40 Gbps (Optional).
16. **(Optional) Dark Fiber**. Dark Fiber shall support the following capabilities:
    a) Deployed fiber shall support both single-mode and multimode fibers.
    b) Deployed fibers shall be capable of supporting a minimum of 80 DWDM wavelengths or user data with spacing as specified in ITU-T G.694.1.
    c) Deployed fibers shall be capable of operating in the "C", ”D”, “L” and ”S” bands.
17. **Digital Subscriber Line** (DSL) Access Arrangements:
    a) Provide the following types of DSL services, at a minimum:
        1. Asymmetric DSL (ADSL). Support ADSL asymmetric data rates for upstream and downstream traffic as follows:
            - Upstream: Data rates shall range from 16 to 768 kbps (e.g., 256 kbps).

- Downstream: Data rates shall range from 1.5 Mbps to 8 Mbps (e.g., at 1.5, 2, 3, 4, 5, 6, 7, and 8 Mbps). Speeds up to 50 Mbps are optional.

2. Symmetric DSL (SDSL). Support SDSL symmetric (i.e., same) data rates for both upstream and downstream traffic at data rates up to and including 1.5 Mbps. 2.3 Mbps is optional
3. (optional) ISDN DSL (IDSL). Support ISDN symmetric (i.e., same) data rates for both upstream and downstream traffic at data rates of 144 Kbps.

18. **Ethernet** Access Arrangements:

a) Ethernet Access Arrangements shall support both dedicated access and/or shared access (multiplexed Ethernet connections) over a Metro Ethernet service from SDP to POP. The contractor shall support access speeds of:

1. 1 Mbps to 10 Mbps at 1 Mbps increments
2. 10 Mbps to 100 Mbps at 10 Mbps increments
3. 100 Mbps to 1 Gbps at 100 Mbps increments
4. (Optional) 2 Gbps to 10 Gbps at 1 Gbps increments
5. (Optional) 10 Gbps to 100 Gbps at 10 Gbps increments

For each of the access connections, the contractor shall maintain appropriate committed bandwidth or CIR (Committed Information Rate), as supported by the MEF 33 - Ethernet Access Services standard and the MEF Bandwidth Profiles for Ethernet Services and as specified in the TO.

19. **(Optional) Cable High-Speed** Service Access Arrangements:

a) Provide data rates of 256 Kbps to 150 Mbps as follows:

1. From 256 Kbps to a maximum of 5 Mbps (Standard: DOCSIS 1.0)
2. From 256 kbps to a maximum of 10 Mbps (Standard: DOCSIS 1.1)
3. From 256 kbps up to 150 Mbps (Standard: DOCSIS 3.0)

20. **(Optional) Fiber-To-The-Premises (FTTP)**:

a) 5 Mbps (downstream) and 2 Mbps (upstream)
b) 15 Mbps (downstream) and 2 Mbps (upstream)
c) 30 Mbps (downstream) and 5 Mbps (upstream) and to a maximum of 150 Mbps (Standard: DOCSIS 3.0)

21. **Wireless** Access Arrangements:

a) Cellular Service - 4G Long Term Evolution (LTE):

1. 100 mbps (downstream) and 50 mbps (upstream)

b) Line of sight connection, using licensed frequencies:
   1. DS1
   2. NxDS1 (where N=2 through 27)
   3. DS3
   4. E1 (Non-domestic)
   5. NxE1 (where N=2 through 15) (Non-domestic)
   6. E3 (Non-domestic)
   7. SONET OC-3
   8. 1 Gbps, 5 Gbps and 10 Gbps

C.2.9.2 Access Diversity and Avoidance

The following are mandatory unless marked optional.

ID Number	Name of Access Capability	Description
1	Access Route or Path Diversity	The contractor shall supply at least two physically-separated routes for access diversity with the following options: 1. Between an SDP and its associated connecting network's PCL or POP, or 2. Between an SDP and at least two connecting network PCL/POPs. 3. Access from the same or different access providers (e.g., ILEC and a CLEC) for two separate routes, using any mix of access arrangements. These diverse routes shall: 1. Not share any common telecommunications facilities or offices including a common building entrance. 2. Maintain a minimum separation of 30 feet throughout all diverse routes between premises/buildings where an SDP and its associated network connecting point are housed. 3. Maintain a minimum vertical separation of two feet, with cables encased (separately) in steel or concrete for cable crossovers. The contractor shall provide the capability for the automatic switching of transmission in real-time, negotiated on an individual case basis: 1. From the primary access route to the one or more diverse access routes, including satellite connection, and 2. From the diverse access route to the primary access route.

ID Number	Name of Access Capability	Description
		The contractor shall exercise the following control measures on the configuration or the reconfiguration of the diverse access route: 1. The contractor shall provide a graphical representation (e.g., diagrams, maps) of access circuit routes to show where diversity has been implemented to the OCO within 30 calendar days of the implementation of access diversity and again thereafter when a change is made. 2. Prior to any proposed reconfiguration of routes previously configured for access diversity, the contractor shall provide to the agency written notification and revised PCLs for OCO approval in accordance with the requirements of the TO. 3. The contractor shall establish internal controls to prevent the dismantling of diversified routes.
2	Access Route or Path Avoidance	The contractor shall supply the capability for a customer to define a geographic location or route to avoid between an SDP and its associated connecting network point. The contractor shall exercise the following control measures on the configuration or reconfiguration of the avoidance access route: 1. The contractor shall provide a graphical representation (e.g., diagrams, maps) of access circuit routes to show where avoidance has been implemented to the OCO within 30 calendar days of the implementation of avoidance and again thereafter when a change is made. 2. Prior to any proposed reconfiguration of routes previously configured for avoidance, the contractor shall provide to the agency written notification and revised PCLs for OCO approval in accordance with the requirements of the TO. 3. The contractor shall establish internal controls to prevent the dismantling of avoided routes.

C.2.9.3 Interfaces

The UNIs at the SDP for AA are mandatory unless marked optional:

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	ITU-TSS V.35	Up to 1.92 Mbps	Transparent
2	EIA RS-449	Up to 1.92 Mbps	Transparent
3	EIA RS-232	Up to 19.2 kbps	Transparent
4	EIA RS-530	Up to 1.92 Mbps	Transparent

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
5	T1 (with ESF) [Std: Telcordia SR-TSV-002275; ANSI T1.403)	Up to 1.536 Mbps	1. Transparent 2. IP (v4/v6)
6	ISDN PRI (23B+D and 24B+0D) [Std: ANSI T1.607/610]	Up to 1.472 Mbps	Transparent
7	T3 [Std: Telcordia GR-400-CORE]	Up to 43.008 Mbps	Transparent
8	E1 (Std: ITU-TSS	Up to 1.92 Mbps G.702) (Non-domestic)	Transparent
9	E3 (Std: ITU-TSS G.702) (Non-domestic)	Up to 30.72 Mbps	Transparent
10	SONET OC-3 (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
11	SONET OC-3c (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
12	SONET OC-12 (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
13	SONET OC-12c (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
14	SONET OC-48 (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
15	SONET OC-48c (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
16	SONET OC-192 (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent
17	SONET OC-192c (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
18	SONET OC-768 (Std: ANSI T1.105 and 106)	38.486016 Gbps	Transparent
19	SONET OC-768c (Std: ANSI T1.105 and 106)	38.486016 Gbps	Transparent
20	10 Base-T/TX/FX (Std: IEEE 802.3)	Link bandwidth: Up to 10 Mbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
21	100 Base-TX/FX (Std: IEEE 802.3)	Link bandwidth: Up to 100 Mbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
22	1000 Base-T/L/LX/B/BX/PX (Std: IEEE 802.3)	Link bandwidth: Up to 1 Gbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
23	10 Gbps (Std: IEEE 802.3)	Link bandwidth: Up to 10 Gbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
24	Reserved		
25	ISDN BRI (2B+D) (Multirate) [Standard: ANSI T1.607 and 610]	144 kbps	1. ITU-TSS Q.931 2. IP (v4/v6)
26	3G / 4G / 4G LTE (Cellular Service)	Up to current standard	1. ITU 3GPP TR25.913 2. IP (v4/v6)

C.2.10 Service Related Equipment

When identified in a TO, the contractor shall provide networking and security service-related equipment such as Switches, Routers, PBXs, Telephones, Servers, Security Appliances, Firewalls, Conferencing-Related Equipment, Microwave Systems, Free-space Optics Systems, Surveillance Systems, Sensors, Radio-related Equipment, VSATs, and Wireless Devices.

The contractor shall provide hardware and materials that are incidental to the installation, operation and maintenance of EIS services.

All equipment provided to the government under this contract shall be new and not previously used or refurbished.

C.2.10.1 Warranty Service

The contractor shall provide, at no additional cost to the government, a minimum one-year system warranty (or the warranty provided by the OEM, whichever is longer) for all hardware and software ordered under this contract, including all equipment supplied, installed, and integrated by the contractor. The equipment warranty shall provide for hardware repairs and the distribution of updated software to all users who ordered the hardware or software under this contract. The contractor shall provide warranty information associated with each product and service delivered to the GSA CO or OCO if requested.

The contractor shall repair or replace malfunctioning equipment covered by warranty within five (5) business days or as specified in the TO. The contractor shall provide to the government a point of contact for the warranty who is available from 7AM – 7PM local time, or for a longer period if specified in the TO. The warranty shall begin at the time the SRE is accepted.

C.2.11 Service Related Labor

The EIS services defined in Sections C.2.1 through C.2.10 and in Section C.2.12 include all service-related labor necessary to implement the services. Agencies may include labor on TOs to support services on this contract. Labor for construction, alteration, and repair is only in-scope as necessary to offer a complete solution, provided that such labor is integral to and necessary for the effort defined in the TO.

C.2.12 Cable and Wiring

The contractor shall provide installation services for equipment necessary to provide telecommunications services and related supporting IT services.

The contractor shall provide required connectivity using appropriate cabling and wiring, and related trenching, ducting, grounding, and lightning protection systems in accordance with the TO and appropriate standards.

Site preparation work done by the contractor under this contract shall conform to applicable federal, regional and local codes and shall conform to accepted industry installation and construction practices. All planned work and code compliance shall be subject to OCO review and approval prior to the start of work. The contractor shall provide the tools and test equipment to perform the site preparation as specified in the

TO, and shall retain ownership of the tools and test equipment unless otherwise specified in the TO. The government will furnish facilities and utilities to the contractor that already are installed at the site, including light, heat, ventilation, and power. The contractor shall provide temporary utilities that are not available in the work area and coordinate any disconnection of utilities. The contractor shall provide building additions and/or changes as required to support the telecommunications and IT installation, provided they are integral to and necessary for the effort defined in the TO. HVAC and electrical construction shall be limited to new or upgraded installations necessary to support telecommunications and IT equipment. The contractor shall expand or modify power systems to provide appropriate environmental controls to support the installation.

The contractor shall provide a warranty period of at least one (1) year for the premises wiring/cabling after service acceptance.

C.3 Transition

In the general sense of the term “transition,” the government can move active services to EIS from any contract or agreement other than EIS, or from EIS to another contract or agreement. However, for the purposes of the EIS program, transition is more narrowly and specifically defined to allow clear and effective tracking of transition progress from certain expiring contracts. Therefore, EIS addresses two types of transition, “transition on” and “transition off,” which are defined as follows:

1. “Transition on” is the transfer of service from a Networx contract or a GSA Local Services Agreement (LSA) to the EIS contract.
2. “Transition off” is the transfer of service from the EIS contract to a follow-on contract or service arrangement, managed by GSA in a coordinated way to prepare for the expiration of the EIS contract, conducted as specified in FAR Clause 52.237-3.

C.3.1 Transition Roles and Responsibilities

C.3.1.1 Government’s Role in Transition

GSA will oversee transition activities to ensure they are progressing and issues are escalated as needed. The functions to be performed by GSA include the following:

1. Develop and publish a Transition Strategy and Management Plan (TSMP) for all stakeholders to have a common understanding of the goals of transition and GSA’s approach to managing transition across the government.
2. Monitor contractor’s performance according to the Transition Management Approach of the Program Management Plan (Section G.9.4) and initiate corrective action if required.
3. Support agencies as resources permit, according to an agreed-upon approach to transition assistance.
4. Coordinate with contractors and agencies to guide the sequence of transition orders to achieve early progress, level resource demands, and minimize backlogs.
5. Track and report on transition progress to all stakeholders and initiate corrective action as required.
6. Monitor and facilitate coordination and cooperation among the contractor, agencies, and other GSA contractors.

The agency will manage EIS transition activities to ensure that replacement services and disconnects are being implemented in a timely and effective manner, with minimal

impact to the agency's operation. Many government organizations are decentralized; therefore, multiple entities within a department or an independent agency may perform the functions of an "agency." The agency's responsibilities and functions may be delegated to another agency, to a sub-agency or an agency component, or to a support contractor authorized to act on behalf of the agency. The functions to be performed by the agency for transition include the following:

1. Validate existing inventory to ensure it is accurate and current.
2. Evaluate current technical solutions and develop transition planning for target technical solutions, including upgrades, transformations, retirement, or other changes.
3. Develop an Agency Transition Plan and identify transition manager(s).
4. Communicate transition goals, telecommunications requirements, and existing inventory to the contractor throughout the ordering process, including within agency solicitations.
5. Monitor the contractor's transition performance, accept or reject services in accordance with Section E Inspection and Acceptance, and coordinate corrective actions with the contractor and GSA if required
6. Monitor and facilitate coordination between the contractor and Local Government Contacts (LGCs) and other agency vendors and service providers.

C.3.1.2 Contractor's Role in Transition

The contractor shall manage transition activities as described in its Program Management Plan. Except where specified further in this section, the contractor shall deliver all services transitioning onto EIS and disconnect services transitioning off EIS according to the same ordering and performance requirements the EIS contract specifies for those services.

C.3.2 Transition On

C.3.2.1 Objectives

GSA expects to define a phased approach for an orderly transition that completes within three (3) years of award of the contract. Furthermore, GSA intends to encourage agencies to enhance or transform services as well as to order new services in conjunction with transitioning services. Therefore, GSA will not require agencies or contractors to identify orders specifically as "transition." Rather, the contractor should ascertain through its order processing practices which services on an order are replacing active services on another contractual vehicle, and give those orders the

appropriate attention to minimize impact on the ordering agency's operations when cutting over to the replacement service.

C.3.2.2 Contract-Wide Planning and Implementation

The contractor shall participate in planning with GSA and conduct transition planning and implementation that are consistent with GSA's TSMP to the extent possible. Certain phases may necessitate contractor personnel being dedicated to focus on those phases and interact with dedicated government personnel. As required by GSA for a phase, the contractor shall identify its personnel by name and contact information. The contractor shall train or orient GSA's transition personnel to use any self-help tools or systems the contractor makes available to agencies for transition and implementation.

C.3.2.3 Agency-Specific Planning and Implementation

The contractor shall respond to agency solicitations with solutions that best address the requirements of the agency to replace its existing services with solutions of equal or better levels of performance, ease of use, and cost effectiveness. The contractor should consult with the agency as appropriate throughout the acquisition process to determine the most effective method of transitioning from existing services to replacement services on EIS, while minimizing impact to the agency's operations. The contractor shall assist ordering agencies with placing TOs and service orders to ensure accuracy, completeness, and timeliness and to minimize delays in transitioning. The contractor shall coordinate with all incumbent contractors according to industry best practices.

C.3.2.4 Inventory

Each agency will compile its own transition inventory of existing services provided by the incumbent contractor. GSA will share with the agency any available information regarding those services and assist the agency in collecting and validating its inventory.

C.3.3 Transition Off

C.3.3.1 Objectives

This section describes the requirements for transitioning services from this contract to a follow-on vehicle.

C.3.3.2 Planning and Implementation

The contractor shall conduct transition planning with GSA and provide advice on strategies to minimize the transition time. The contractor shall perform PIC/LPIC changes in support of transition from EIS to a follow-on contract. The contractor shall accept a Letter of Authorization (LOA) from the agency to allow the follow-on contractor to order PIC/LPIC changes, including release of PIC freeze.

C.3.3.3 Inventory

In preparation for transition off this contract, the government must have a complete and accurate Transition Inventory. A Transition Inventory is a complete record of the services, features, equipment, location data, configuration information, and delivery description necessary to facilitate the transition of an agency's services. For solutions with delivery details that are more transparent to the user – such as TUCs, managed services, or cloud services – the delivery description shall include the functional solution and performance specification of the service rather than specific components.

If GSA exercises all the contract options, for the final five (5) years of the contract, the contractor shall conduct periodic validations (approximately once every 6 months) of its Transition Inventory with GSA and reconcile any discrepancies. If GSA exercises all the contract options, for the final three years of the contract the contractor shall conduct monthly validations with GSA. At the GSA CO's request, the contractor shall deliver an inventory summary of all services active – that is, in service, whether in use or not – at the time of the request, by AB code, service, quantity, and location. At the OCO's request, the contractor shall deliver an inventory summary of all the agency's services active at the time of the request.

C.3.3.4 Reporting

If GSA exercises all the contract options, for the final three (3) years of the contract, the contractor shall deliver weekly reports of services disconnected and active services based upon the transition inventory.

During that same three-year period the contractor shall deliver a monthly Transition Status Report that includes the following:

- Data file of invoiced amount by AB code for the most recently completed billing period
- Discussion of transition issues reported by agency customers or experienced by the contractor either during the reporting period or unresolved since the last report, corrective action, and status
- Risk analysis and response plan.

C.4 Section 508 Requirements

C.4.1 Background

Section 508 is the statutory section of the Rehabilitation Act of 1973 that requires federally procured Electronic Information Technology (EIT as defined in FAR 2.101) to provide disabled federal employees with access to and use of information that is comparable to information provided to nondisabled federal employees. Section 508 also requires federal agencies to provide disabled public citizens with access to and use of information that is comparable to information provided to nondisabled public citizens. For additional information see www.section508.gov.

The Access Board is an independent federal agency that established the standards for federally procured EIT products and services. The requirements that must be met consist of Technical Standards ~~(Section 508, Subpart B)~~, Functional Performance Criteria ~~(Section 508, Subpart C)~~, and Information, Documentation, and Support ~~(Section 508, Subpart D)~~.

Agencies may accept EIT that uses designs and/or technologies that do not meet applicable Technical Standards ~~of Subpart B~~ but do provide disabled federal employees or citizens with equivalent or greater access to information. This is referred to as "equivalent facilitation" and vendors offering equivalent facilitation will be considered along with those that strictly meet the Technical Standards ~~of Subpart B~~.

Revised Standards –As of January 18, 2018, Federal agencies must comply with the revised 508 Standards, which were issued by the U.S. Access Board in January 2017. These revised standards are set forth in 36 C.F.R. § 1194.1 and Appendices A, C and D to Part 1194. Information and communication technology (ICT) developed, maintained, or used by Federal agencies on or after this date must satisfy the updated scoping and technical requirements in the Revised 508 Standards. These Standards may be found at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines

Safe Harbor - The Revised 508 Standards also include a "safe harbor" provision for existing (i.e., legacy) ICT. Under this safe harbor, unaltered, existing ICT (including electronic content) that complies with the Original 508 Standards need not be modified or upgraded to conform to the Revised 508 Standards. This safe harbor applies on an element-by-element basis to each component or portion of the existing ICT, with each component or portion assessed separately. Existing, unaltered ICT that did not comply with the Original 508 Standards as of January 18, 2018 must now be brought into compliance with the Revised 508 Standards.

C.4.2 Voluntary Product Accessibility Template

The contractor shall post the Voluntary Product Accessibility Template (VPAT) for each service identified in paragraphs C.4.4 below to its web site, in order to demonstrate that offerings comply with Section 508 standards. The VPAT is required 30 days after NTP and is updated as needed. This will assist the customer agency in evaluating services for Section 508 standard compliance.

C.4.3 Section 508 Applicability to Technical Requirements

The Technical Requirements section (Section C.2) of the contract identifies the technical provisions for services used by an agency to execute mission operations. Services that execute mission operations shall meet the relevant provisions of ~~Section 508, Subparts B, C, and D~~ as identified in Section C.4.4 or shall provide equivalent facilitation. For less than fully compliant products see Section G.5.3.1.3.

C.4.4 Section 508 Provisions Applicable to Technical Requirements

The relevant provisions of Part 1194 Appendix A Chapter 1 Application and Administration and Chapter 2 Scoping Requirements along with Part 1194 Appendix C Chapter 3 Functional Performance Criteria , Chapter 4 Hardware, Chapter 5 Software, Chapter 6 Support Documentation and Services, and Chapter 7 Referenced Standards~~Subpart B, Technical Standards, paragraph 1194.21 , Software Applications and Operating Systems~~, shall apply to the appropriate EIS software,hardware, and web-based services, to include but not be limited to the following:

- Data Service.
- Voice Service.
- Managed Service.
- Contact Center Service.
- Data Center Service.
- Cloud Service.

~~The relevant provisions of Subpart B, Technical Standards, paragraph 1194.22, **Web-based Intranet and Internet Information and Applications,** shall apply to the appropriate EIS services, to include but not be limited to the following:~~

- ~~Data Service.~~
- ~~Managed Service.~~
- ~~Contact Center Service.~~
- ~~Data Center Service.~~

Formatted: Default Paragraph Font, Font: Arial, 12 pt, Font color: Auto, Border: : (No border), Pattern: Clear

Formatted: Default Paragraph Font, Font: Arial, 12 pt, Font color: Auto, Border: : (No border), Pattern: Clear

Formatted: Font: Not Bold

Formatted: Default Paragraph Font, Font: Arial, 12 pt, Font color: Auto, Border: : (No border), Pattern: Clear

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

- ~~Cloud Service.~~

~~The relevant provisions of Subpart B, Technical Standards, paragraph 1194.23, **Telecommunications Products**, shall apply to the appropriate EIS services, to include but not be limited to the following:~~

- ~~Voice Service.~~
- ~~Data Service.~~
- ~~Managed Service.~~
- ~~Contact center Service.~~
- ~~Data Center Service.~~
- ~~Cloud Service.~~

The relevant provisions of ~~Subpart C~~Part 1194 Appendix C Chapter 3, Functional Performance Criteria, ~~paragraph 1194.31,~~ shall apply to appropriate services provided under the EIS contract. For the relevant services, the contractor shall provide one of the following two capabilities:

1. Support for assistive technologies used by disabled individuals.
2. At least one mode of operation and information retrieval that:
   a) For blind users, does not require vision.
   b) For vision impaired users, does not require visual acuity greater than 20/70.
   c) For deaf users, does not require hearing.
   d) For hearing impaired users, does not require enhanced auditory capability.
   e) For users with no speech capability or with impaired speech, does not require user speech.
   f) For users without fine motor control or simultaneous action capability, does not require fine motor control or simultaneous action and is operable without limited reach and strength.

The relevant provisions of ~~Subpart D, Information, Documentation, and Support, paragraph 1194.41~~ Part 1194 Appendix C Chapter 6 Support Documentation and Services, shall apply to the appropriate services provided under the EIS contract.

Formatted: Default Paragraph Font, Font: Arial, 12 pt, Font color: Auto, Border: : (No border), Pattern: Clear

C.4.5 Section 508 Provisions Applicable to Reporting and Training

The government's information reporting requirements are addressed in Section G.9 Program Management. Required information shall be reported via the Internet, email, or telephone. Services providing the required information shall meet the relevant

provisions of ~~Section 508, Subparts B, C, and D~~ Part 1194 Appendices A and C or shall provide equivalent facilitation.

Training requirements are outlined in Section G.10 Training shall be delivered via meeting and briefings, classroom, seminars, instructor-led and non-instructor on-line web based self-study, and manuals or desk top guides. For training delivered via meeting and briefings, classroom, and seminars, assistance such as signers and Braille products shall be provided to disabled trainees when requested in advance by the government. For training delivered via instructor-led and non-instructor on-line web based, the same capabilities provided for Internet reporting shall be provided to disabled trainees.

Enterprise Infrastructure Solutions (EIS)
Request for Proposals

Section D
Packaging and Marking

Issued by:

General Services Administration

Office of Integrated Technology Services

(b) (2) [redacted]

[redacted]

JULY 2017

Table of Contents

D.1 Preservation, Packaging and Packing

Unless otherwise specified, all items shall be preserved, packaged, and packed in accordance with normal commercial practices, as defined in the applicable commodity specification. Packaging and packing shall comply with the requirements of the Uniform Freight Classification and the National Motor Freight Classification (issue in effect at time of shipment) and each shipping container or each item in a shipment shall be of uniform size and content, except for residual quantities. Where special or unusual packing is specified in a task order, but not specifically provided for by the contract, such packing details must be agreed to by the ordering agency and the contractor.

D.2 Packing List

A packing list or other suitable shipping document shall accompany each shipment and shall indicate:

1. Name and address of the consignor
2. Name and complete address of the consignee
3. Government order or requisition number
4. Government bill of lading number covering the shipment (if any)
5. Description of the material shipped, including item number, quantity, number of containers, package number (if any), and weight of each package

D.3 Initial Packing, Marking, and Storage of Equipment

All initial packing, marking and storage incidental to shipping of equipment to be provided under this contract shall be made at the contractor's expense. Such packing, supervision marking and storage costs shall not be billed to the government. Supervision of packing and unpacking of initially acquired equipment shall be furnished by the contractor.

D.4 Equipment Removal

All leased equipment, accessories, and devices located on government property shall be dismantled and removed from government premises by the contractor, at the contractor's expense, within 45 days after the service termination date. All dismantling and removal of equipment shall be performed by the contractor during normal government business hours at the location. Advance notice must be provided to the Local Government Contact to ensure that such dismantling and removal occurs with a minimum of disruption. Exceptions to this requirement shall be mutually agreed upon and written notice issued by the agency Ordering Contracting Officer.

Enterprise Infrastructure Solutions (EIS)

Contract

Section E

Inspection and Acceptance

Issued by:

General Services Administration

Office of Information Technology Category

(b) (2), (b) (4)

[redacted]

September 2017

Table of Contents

E.1 Introduction

This section describes the inspection and acceptance plan for the following:

- Contractor's Business Support Systems (BSS)
- EIS Services

E.1.1 FAR 52.252-2 Clauses Incorporated by Reference (FEB 1998)

This contract incorporates one or more FAR clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer (CO) will make their full text available. The full text of a clause may be accessed electronically at this address: www.acquisition.gov/far.

The clauses in Table E.1.1.1 apply at the contract and order levels, as applicable, depending upon the contract type of the order, or as specifically referenced in the applicable order.

E.1.1.1 Clauses Incorporated by Reference Table

Clause #	FAR Clause #	Title and Date	Date
E.1.1	52.246-2	Inspection of Supplies - Fixed Price	AUG 1996
E.1.2	52.246-4	Inspection of Services - Fixed Price	AUG 1996
E.1.3	52.246-6	Time-and-Material and Labor-Hour	MAY 2001
E.1.4	52.246-12	Inspection of Construction	AUG 1996
E.1.5	52.246-16	Responsibility for Supplies	APR 1984
E.1.6	52.246-17	Warranty of Supplies of a Noncomplex Nature	JUN 2003
E.1.7	52.246-19	Warranty of Systems and Equipment under Performance Specifications or Design Criteria	MAY 2001
E.1.8	52.246-20	Warranty of Services	MAY 2001

E.2 Test Methodology

The contractor shall follow the verification and acceptance test methodology described in this section in developing the verification test plan(s) for:

- Contractor's Business Support Systems (BSS)
- EIS Services

E.2.1 Business Support Systems Verification Testing

The contractor shall provide a draft BSS Verification Test Plan (BSS Test Plan) with its proposal and a final BSS Test Plan 30 days after notice to proceed. This plan shall comply with the test methodology for BSS defined in Sections E.2.1.1 – E.2.1.5. The government reserves 21 days from the date of receipt of final plan to accept or reject the plan. If it is rejected, the contractor will be given the opportunity to update the plan based on government comments.

Based on GSA Conexus readiness and other factors, the government may, at its option, offer the opportunity for contractors to perform preliminary testing prior to award, but after submission of proposals. If this opportunity is offered, it will be offered to all contractors who submit a proposal, pending only the contractor's demonstration of primary security features such as anti-virus protection. Any such preliminary testing shall not replace formal testing post-award. The government offers no guarantees that the GSA Conexus configuration offered as the preliminary system will be identical to the final system used in post-award formal testing. If the government offers such preliminary testing, the government will issue terms and conditions for such testing which the contractor must accept prior to accessing the test system.

The contractor shall provide updates to the BSS Test Plan within 14 days of receipt of government comments. The government reserves 14 days after receipt of the updated plan to accept or reject it. If necessary to gain approval, the contractor may repeat this process.

See section G.2.3 BSS Final Contract Acceptance for final acceptance requirement.

In support of BSS testing, GSA will provide test parameters as follows: BSS test scenarios are provided in Section E.2.1.2. BSS test cases are provided in Section E.2.1.3. Test metadata (including approximate number of TOs, SOs, and other data sets to be used in testing) will be provided not later than NTP. System reference data, as described in Section J.2.3, will be provided not later than NTP. Test data, as described in Section E.2.1.3, and test verification criteria will be provided at the time of BSS testing.

The BSS testing will be performed during normal business hours, 8:00am-5:00pm Monday-Friday, Eastern Time.

E.2.1.1 Scope

The contractor shall meet the following Inspection and Acceptance requirements:

- BSS testing shall verify that all BSS functional, regression and security requirements have been successfully met.
- BSS testing shall be performed for all management and operation functions supporting Ordering, Billing, Inventory Management, Disputes, SLA Management and Trouble Ticketing processes described in Section G and Section J.2.
- Security testing shall be based on the requirements described in Section G.5.6 BSS Security Requirements. The security requirements acceptance shall be based on:
    - Assessment and Authorization (A&A)
    - FedRAMP certification (if applicable)
- BSS testing shall include multiple test cases that are defined in Section E.2.1.3 Test Cases.
- BSS testing shall include test cases for quality, utility and customer access features.
- The contractor shall allow government representative(s) to observe all or any part of the verification testing.
    - If the government so requests, the contractor shall perform tests to ensure continued compliance each time a new service is offered or the contractor modifies features/functionality of the BSS that affect the functional requirements described in Section G and Section J.2.
- The contractor shall perform BSS verification testing according to the accepted BSS Test Plan at a mutually acceptable date with the government.

E.2.1.2 BSS Test Scenarios

E.2.1.2.1 Testing Prerequisites

Prior to initiating BSS testing, the contractor shall:

- Provide written notice to the government that the contractor's BSS has passed its internal testing and is ready to begin BSS interface testing with GSA Conexus.
- Provide a finalized BSS Test Plan that is accepted by GSA.

The purpose of the verification and acceptance testing is to ensure that the contractor's BSS meets requirements in Section G and Section J.2. The contractor shall support

BSS security and functional testing as defined in Section G.5.6 BSS Security Requirements and Section G.2.3 BSS Final Contract Acceptance.

E.2.1.2.2 Test Scenarios

The following table contains a high-level list of BSS Test Scenarios for which the contractor's BSS must pass the defined acceptance criteria. The contractor shall address the test scenarios based on the functional requirements defined in the relevant portions of Section G and/or Section J.2 (see the "RFP References" column for references).

The scenarios shall address relevant data exchange mechanisms and validation of data exchanged. Each Test Scenario is associated with one or more Test Cases defined in Section E.2.1.3.

Test Scenario #	RFP References	Description	Acceptance Criteria
BSS-TS01	• G.5.3.2 • J.2.9	Exchange structured data using the defined direct data exchange methods: • XML via secure web services • Pipe, "|", delimited table via SFTP	The contractor shall demonstrate bidirectional exchange of defined data structure that meets the interface specifications as defined in Section G.5.3.2 and Section J.2.9.
BSS-TS02	• G.3 • J.2.3	The contractor's BSS manages the following as specified in Section J.2.3: • Accept System Reference Data • Provide Direct Billed Agency Setup	The contractor shall demonstrate successful TO Data Management initial setup and updates.
BSS-TS03	• J.2.3	The contractor's BSS manages Role based access control to all BSS functions (e.g. ordering, billing, inventory management, trouble management, SLA management)	The contractor shall demonstrate that its BSS provides the ability to define role based users with privileged access to the BSS to meet the requirements as defined in Section J.2.3.
BSS-TS04	• G.3 • J.2.4	The contractor's BSS manages the processing of orders and generation of required acknowledgments and notifications. Order types include: • New service for each of the services specified in Section C.2, Technical Requirements, that are included in the awardee's contract • Service Moves • Service Disconnects • Service Feature Changes	The contractor shall demonstrate that an authorized government user can place an order using the methods specified in Section J.2.4 and the order populates the fields in the contractor's BSS in a way that meets the requirements in Sections G.3, G.5 and J.2. Using the direct data exchange method defined in Section J.2.4, the contractor shall demonstrate that its BSS can provide all required CDRLs including:

Test Scenario #	RFP References	Description	Acceptance Criteria
		• Telecommunications Service Priority (TSP) • Auto-sold CLINs • Bulk Orders	1) Service Order Acknowledgement 2) Service Order Rejection Notice 3) Service Order Confirmation 4) Firm Order Commitment Notice 5) Service Order Completion Notice
BSS-TS05	• G.3 • J.2.4	The contractor's BSS handles order supplements/updates that impact other, in-progress orders: • Cancel orders • Service Feature Changes • Location changes • Changes to Customer Want Date • Changes to administrative data	The contractor shall demonstrate that an authorized government user can place a change or cancel order using the methods specified in Section J.2.4 and the order populates the fields in the contractor's BSS in a way that meets the requirements in Sections G.3, G.5 and J.2. Using the direct data exchange method defined in Section J.2.4, the contractor shall demonstrate that its BSS can provide all required CDRLs including: 1) Service Order Acknowledgement 2) Service Order Rejection Notice 3) Service Order Confirmation 4) Firm Order Commitment Notice 5) Service Order Completion Notice
BSS-TS06	• G.3 • J.2.4	The contractor's BSS handles orders for administrative changes to the records for previously provisioned services as described in G.3	The contractor shall demonstrate that an authorized government user can place an administrative change order using the methods specified in Section J.2.4 and the order populates the fields in the contractor's BSS in a way that meets the requirements in Sections G.3, G.5 and J.2. Using the direct data exchange method defined in Section J.2.4, the contractor shall demonstrate that its BSS can provide all required CDRLs including: Service Order Administrative Change
BSS-TS07	• G.3.5.6 • J.2.4.2.4	The contractor's BSS manages Self-Service Provisioning and other Rapid Provisioning orders and provides the correct notices.	The contractor shall successfully demonstrate the completion of these orders. Non-self-service orders shall be tested using both correctly placed orders and orders with related errors. Self-service orders

Test Scenario #	RFP References	Description	Acceptance Criteria
			shall be tested with correctly placed orders and to ensure that the contractor's BSS does not permit the placement of incorrect orders. Using the direct data exchange method defined in Section J.2.4, the contractor shall demonstrate that its BSS can provide all required CDRLs including: 1) Service Order Acknowledgement 2) Service Order Completion Notice
BSS-TS08	• G.4 • J.2.5 • J.2.6 • J.2.7 • J.2.10	The contractor's BSS properly manages inventory and billing: • Generates the inventory of services delivered by the contractor • Produces output that is consistent with order and billing details • Generates the detailed billing in accordance with the Billing Invoice (BI) CDRL • Properly handles usage-based billing • Calculates billing based on the contractor's awarded pricing • Correctly calculates the AGF due to GSA and produces the required AGF CDRLs • Provides accurate calculation of rounding and proration related to Billing, Taxes, Fees and Surcharges	The contractor shall demonstrate that its service inventory management system maintains a complete and accurate inventory of EIS service orders in a way that meets the requirements in G.7 and G.5 and Section J.2 CDIP and is verified and accepted by GSA. The contractor shall demonstrate that the output of its billing data elements is consistent with the orders entered into its BSS and that the billing data elements meet the requirements in Sections G.3, G.5 and J.2. Using the direct data exchange method defined in Sections J.2.5-J.2.7, the contractor shall demonstrate that its BSS can provide all required CDRLs including: 1) Billing Invoice 2) Billing Adjustment 3) Tax Detail 4) AGF Detail 5) AGF Electronic Funds Transfer Report 6) Inventory Reconciliation
BSS-TS09	• G.4.4 • J.2.6	The contractor's BSS properly manages all dispute types with appropriate handling for: • Billing disputes • Inventory disputes • SLA disputes • Dispute tracking and reporting	The contractor shall demonstrate that its BSS can accept and issue disputes as well as tracking them to resolution. Using the direct data exchange method defined in Sections J.2.5-J.2.7, the contractor shall demonstrate that its BSS can

Test Scenario #	RFP References	Description	Acceptance Criteria
			provide all required CDRLs including: 1) Dispute 2) Dispute Report
BSS-TS10	• G.8 • J.2.8	The contractor's BSS properly manages SLA Management: • SLA Reporting • SLA Credit Request handling and response	The contractor shall demonstrate that its BSS successfully tracks SLAs with associated KPIs as well as reporting SLA performance and providing sufficient information to response to SLA Credit Requests. Using the direct data exchange method defined in Sections J.2.5-J.2.7, the contractor shall demonstrate that its BSS can provide all required CDRLs including: 1) SLA Report 2) SLA Credit Request Response
BSS-TS11	• J.2	The contractor's BSS produces acceptable open-format reports defined in the CDIP: • Monthly Billing Information Memorandum • Trouble Management Incident Performance Report • Trouble Management Performance Summary Report	The contractor shall demonstrate, via sample reports, that the open-format reports specified are sufficiently detailed and clear so as to meet the government's requirements.
BSS-TS12	• J.2	The contractor's BSS testing includes regression testing of all key features including ordering, service assurance, and billing. NOTE: Applies only to testing conducted as part of system changes, not initial BSS development.	The contractor shall demonstrate that its BSS meets regression testing. The BSS test plan shall include regression testing; however, actual regression testing will not be part of initial test and acceptance.
BSS-TS13	• G.5.6	The contractor's BSS has passed A&A as defined in Section G.5.6.	The contractor shall demonstrate that the BSS meets FISMA Moderate requirements.

E.2.1.3 BSS Test Cases

The contractor shall accept, incorporate into the BSS Test Plan, and successfully execute test cases provided for each of the test scenarios above.

- The contractor shall accept the following test conditions:

- No testing between the contractor and GSA shall occur until both the contractor's BSS and GSA Conexus have passed unit testing.
- All testing to be performed on the actual system to be used in delivering service (i.e. special purpose "test systems" shall not be used).
- Unless otherwise specified, all data transfers are to use the mechanism specified in Section J.2 for that data set.

- The contractor shall use GSA provided test data for all BSS verification testing unless specified otherwise:
  - This data shall be used for testing purposes only.
  - No customer "live" data shall be used for testing.
  - This data shall be a realistic simulation of actual customer data.
  - The test data shall include, in some tests, intentional errors intended to test the contractor's BSS error handling.
- BSS testing shall follow a tiered approach:
  - The contractor shall accept multiple test cases for the test scenarios defined in Section E.2.1.2.
  - The contractor shall accept, incorporate into the BSS Test Plan, and successfully execute each test case with one or more test data sets.
  - In providing test data sets, GSA will group them into Test Subcases:
    - Each Test Subcase shall contain data sets intended to test a specific "real world" test case (e.g. a complete and accurate disconnect order)
    - Each test subcase shall include at least two complete test data sets
- BSS functional testing acceptance:
  - The contractor's BSS shall not have completed functional testing until all BSS Test Scenarios (Section E.2.1.2) are passed.
  - A test scenario shall not be considered passed until the contractor's BSS properly handles each associated test case.
  - A test case shall not be considered passed until the contractor's BSS properly handles each associated subcase twice in succession using different data sets.
  - A subcase shall not be considered passed until the contractor's BSS properly handles the data sets following the prescribed actions with no errors or warnings.
- BSS security testing acceptance is defined in Section G.5.6 and associated references.

The individual test cases are defined in the tables in the subsections below. Each test case table includes the following headings:

- Test Scenario: The associated test scenario from Section E.2.1.2.
- Test Case ID: Identification number for the test case.
- Test Case Description: Brief title of the test case.
- Requirements Reference(s): Where the functional requirements that are being tested can be found.
- Prerequisites: Actions that must be completed prior to implementing the test case (in addition to the general prerequisites for all testing).
- Government Input(s): Data the government will provide as input to the test case.
- Expected BSS Output(s): Expected data or actions from the contractor's BSS.
- Data Set Description: Brief description of the data sets the government intends to provide as part of testing.
- Acceptance Criteria: Factors to be checked prior to acceptance of the test results. The table below defines the terms used:

Criteria	Definition
Successful data transfer	The contractor demonstrates that data transmitted was received intact without error using the formats and mechanisms described in the test case.
Correct technical aspects	The contractor demonstrates that data transfers were completed using the correct mechanism, in the correct format, and with the correct structure.
Evidence of failure notification	The contractor demonstrates that expected notifications of failure were properly issued.
No partial import	The contractor demonstrates that their BSS does not import partial data in cases where the data is corrupt or otherwise cannot be imported in full.
All required CDRLs	The contractor demonstrates that the expected CDRLs (listed in the expected output section) are all delivered.
Accurate data based on inputs	The contractor demonstrates that the data provided in CDRLs is accurate and reflects the data provided by the government inputs and the prerequisites.
Access granted	The contractor demonstrates that the user gains access to resources as expected.
Access denied	The contractor demonstrates that the user is denied access to resources as expected.
No errors displayed	The contractor demonstrates that the user is not shown any unexpected errors.

Criteria	Definition
Appropriate errors are displayed	The contractor demonstrates that the user is shown the expected errors.
CDRLs are internally consistent	The contractor demonstrates that the data provided in the expected CDRLs is internally consistent between the set of CDRLs.
Complies with calculation rules	The contractor demonstrates that the data provided in the CDRLs matches that which would be expected based on rounding and proration calculation requirements.
Each CDRL meets requirements	The contractor demonstrates that the provided CDRLs meet the requirements specified by the government (used for CDRLs without detailed format requirements). Standard requirements include, at minimum: • CDRL contains the required information • CDRL is clear and readily understood
Contractor BSS receives ATO	The contractor demonstrates that the BSS has received Authorization to Operate (ATO) and has been approved by GSA based on relevant security requirements as defined in Section G.5.6 and references therein.

E.2.1.3.1 BSS-TS01: Direct Data Exchange

E.2.1.3.1.1 BSS-TS01-01: XML over Secure Web Services

Test Scenario	BSS-TS01: Direct Data Exchange
Test Case ID	BSS-TS01-01
Test Case Description	XML over Secure Web Services
Requirements Reference(s)	• G.5.3.2 • J.2.9
Prerequisites	• N/A
Government Input(s)	• Instructions to submit xml over web services will be provided at the time of BSS testing~~Properly formatted government data set listed as using web services as the transfer mechanism in Section J.2~~
Expected Output(s)	• Properly formatted contractor data set that meets the following criteria: ○ Listed as using web services as the transfer mechanism in Section J.2 ○ Includes data derived from the government input
Acceptance Criteria	• Successful data transfer • Correct technical aspects
Data Set Description	~~•~~ N/A ~~Each government-provided test data set will include:~~ • ~~One government data set listed as using web services as the transfer mechanism in Section J.2~~

E.2.1.3.1.2 BSS-TS01-02: PSV over SFTP

Test Scenario	BSS-TS01: Direct Data Exchange
Test Case ID	BSS-TS01-02
Test Case Description	PSV over SFTP
Requirements Reference(s)	• G.5.3.2 • J.2.9
Prerequisites	• N/A
Government Input(s)	• Properly formatted government data set listed as using SFTP as the transfer mechanism in Section J.2
Expected Output(s)	• Properly formatted contractor data set that meets the following criteria: ○ Listed as using SFTP as the transfer mechanism in Section J.2 ○ Includes data derived from the government input
Acceptance Criteria	• Successful transfer of PSV data • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ One government data set listed as using SFTP as the transfer mechanism in Section J.2

E.2.1.3.1.3 ~~BSS-TS01-03: Error Handling: XML over Secure Web Services~~Reserved

~~**Test Scenario**~~	~~BSS-TS01: Direct Data Exchange~~
~~**Test Case ID**~~	~~BSS-TS01-03~~
~~**Test Case Description**~~	~~Error Handling: XML over Secure Web Services~~
~~**Requirements Reference(s)**~~	~~• G.5.3.2~~ ~~• J.2.9~~
~~**Prerequisites**~~	~~• N/A~~
~~**Government Input(s)**~~	~~• Invalid government data set listed as using web services as the transfer mechanism in Section J.2~~
~~**Expected Output(s)**~~	~~• Notification to contractor of failed import~~
~~**Acceptance Criteria**~~	~~• Evidence of failure notification~~ ~~• No partial import~~
~~**Data Set Description**~~	~~• Each government provided test data set will include:~~ ~~○ One government data set listed as using web services as the transfer mechanism in Section J.2~~ ~~○ One or more XML formatting errors (e.g. missing delimiters)~~

E.2.1.3.1.4 BSS-TS01-04: Error Handling: PSV over SFTP

Test Scenario	BSS-TS01: Direct Data Exchange
Test Case ID	BSS-TS01-04
Test Case Description	Error Handling: PSV over SFTP
Requirements Reference(s)	• G.5.3.2 • J.2.9
Prerequisites	• N/A
Government Input(s)	• Invalid government data set listed as using SFTP as the transfer mechanism in Section J.2
Expected Output(s)	• Notification ~~to~~ from the contractor of failed import
Acceptance Criteria	• Evidence of failure notification • No partial import
Data Set Description	• Each government-provided test data set will include: ○ One government data set listed as using SFTP as the transfer mechanism in Section J.2 ○ One or more formatting errors (e.g. missing delimiters)

E.2.1.3.2 BSS-TS02: Task Order Data Management

E.2.1.3.2.1 BSS-TS02-01: Direct Billing Account Setup

Test Scenario	BSS-TS02: Task Order and Account Management Setup
Test Case ID	BSS-TS02-01
Test Case Description	Direct Billing Account Setup
Requirements Reference(s)	• G.3 • J.2.2 • J.2.3
Prerequisites	• N/A
Government Input(s)	• Task order controlled data as defined in Section J.2.3 • Task order associated data as defined in Section J.2.3 • System Reference data as defined in Section J.2.3
Expected Output(s)	• Direct Billed Agency Setup (DBAS) CDRL
Acceptance Criteria	• All required CDRLs as defined in Section J.2.3 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ Sample TO controlled data transferred in the form of a sample TO ○ Sample TO associated data transferred in free format (not previously defined) unless the contractor specifies in their

	proposal that customer registration is to be submitted via their web interface and that interface collects all of the required data ○ Sample System Reference data transferred using the mechanism specified in Section J.2

E.2.1.3.2.2 Reserved

E.2.1.3.3 BSS-TS03: Role Based Access Control

E.2.1.3.3.1 BSS-TS03-01: Authorized User Access Verification

Test Scenario	BSS-TS03: Role Based Access Control
Test Case ID	BSS-TS03-01
Test Case Description	Authorized User Access Verification
Requirements Reference(s)	• G.5 • J.2.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• User attempts to: ○ Sign into BSS ○ Access BSS areas to which they are an authorized user ○ Exercise the full range of functionality (read/write) permitted for their role
Expected Output(s)	• User is permitted to: ○ Access to BSS ○ Access BSS areas as authorized ○ Exercise assigned functionality
Acceptance Criteria	• Access is granted • No security errors displayed
Data Set Description	• Each government-provided test data set will include: ○ Role to be tested ○ Functionality to be tested

E.2.1.3.3.2 BSS-TS03-02: Unauthorized User Access Denial Verification

Test Scenario	BSS-TS03: Role Based Access Control
Test Case ID	BSS-TS03-02
Test Case Description	Unauthorized User Access Denial Verification
Requirements Reference(s)	• G.5 • J.2.3.
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS

Government Input(s)	• User attempts to:
	  ○ Sign into BSS
	  ○ Access BSS areas to which they are not an authorized user
	  ○ Exercise functionality (read/write) not permitted for their role

Expected Output(s)	• User is denied access at the point appropriate the role, area and functionality specified in the test data set:
	  ○ Access to BSS
	  ○ Access to specific BSS areas
	  ○ Access to specific functionality
	• User is shown security error message

Acceptance Criteria	• Access is denied • Appropriate errors are displayed

Data Set Description	• Each government-provided test data set will include:
	  ○ Role to be tested (may be specified as none if the set is intended to show denial of unauthorized users)
	  ○ Functionality to be tested

E.2.1.3.4 BSS-TS04: Service Ordering

E.2.1.3.4.1 BSS-TS04-01: New Order via Web Interface

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-01
Test Case Description	New Order via Web Interface
Requirements Reference(s)	• G.3 • G.5.3.1 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.10.2.1.15
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Service Order Confirmation (SOC) ○ Firm Order Commitment Notice (FOCN) ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO for one or more services listed in Section C.2 of the contract ○ SO to be entered into the contactor's BSS via the contractor's web interface as described in Section G.5.3.1

E.2.1.3.4.2 BSS-TS04-02: New Order via Email

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-02
Test Case Description	New Order via Email
Requirements Reference(s)	• G.3 • G.5.3.1 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.10.2.1.15
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Service Order Confirmation (SOC) ○ Firm Order Commitment Notice (FOCN) ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO for one or more services listed in Section C.2 of the contract ○ SO submitted via a means listed in J.2.4 other than the contractor's web interface

E.2.1.3.4.3 BSS-TS04-03: Disconnect Order

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-03
Test Case Description	Disconnect Order
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.2
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS • Previously provisioned circuit or service element entered into the contractor BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 for the disconnect of ○ A circuit or service element (CLIN) ○ A feature of a circuit or service element
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Service Order Confirmation (SOC) ○ Firm Order Commitment Notice (FOCN) if required based on the requirements described in Section J.2.4 ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO for the disconnect of a circuit or service element or a feature of a circuit or service element as described in Section G.3 and Section J.2.10.1.1.4.2

E.2.1.3.4.4 BSS-TS04-04: Feature Addition Order

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-04
Test Case Description	Feature Addition Order
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.2
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS • Previously provisioned circuit or service element entered into the contractor BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 for the addition of a feature to a circuit or service element
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Service Order Confirmation (SOC) ○ Firm Order Commitment Notice (FOCN) ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO for the addition of a feature to a circuit or service element as described in Section G.3 and Section J.2.10.1.1.4.2

E.2.1.3.4.5 BSS-TS04-05: Move Order

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-05
Test Case Description	Move Order
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.2
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS • Previously provisioned circuit or service element entered into the contractor BSS
Government Input(s)	• Two Service Orders (SOs) that combine to specify the move of a circuit or service element with all required data elements as described in Section J.2.4 ○ One SO for the disconnect of the circuit or service element at the old location ○ Second SO for the installation of the identical circuit or service element at the new location
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Service Order Confirmation (SOC) ○ Firm Order Commitment Notice (FOCN) ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A pair of complete SOs for the move of a circuit or service element from one valid location to another as described in Section G.3 and Section J.2.10.1.1.4.2 ▪ SO for the disconnect from the old location ▪ SO for the installation of the identical service at the new location

E.2.1.3.4.6 BSS-TS04-06: TSP Order

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-06
Test Case Description	TSP Order
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) requesting TSP with all required data elements as described in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Service Order Confirmation (SOC) ○ Firm Order Commitment Notice (FOCN) ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO with a TSP code for one or more services listed in Section C.2 of the contract

E.2.1.3.4.7 BSS-TS04-07: Auto-Sold CLINs

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-07
Test Case Description	Auto-Sold CLINs
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) that includes CLINS with associated Auto-Sold CLINs and contains all required data elements as described in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Service Order Confirmation (SOC) ○ Firm Order Commitment Notice (FOCN) ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO that includes Auto-Sold CLINs for one or more services listed in Section C.2 of the contract

E.2.1.3.4.8 BSS-TS04-08: Task Order Unique CLINs (TUCs)

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-08
Test Case Description	Task Order Unique CLINs (TUCs)
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO setup data loaded into contractor BSS ○ TO Data defines one or more TUCs • Account Management data loaded into contractor BSS
Government Input(s)	• Service Order (SO) containing Task Order Unique CLINs (TUCs) and all required data elements as described in Section J.2.4

Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4:
	  ○ Service Order Acknowledgment (SOA)
	  ○ Service Order Confirmation (SOC)
	  ○ Firm Order Commitment Notice (FOCN)
	  ○ Service Order Completion Notification (SOCN)

Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO containing Task Order Unique CLINs (TUCs) for one or more services listed in Section C.2 of the contract

E.2.1.3.4.9 Reserved

E.2.1.3.4.10 BSS-TS04-10: Bulk Orders

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-10
Test Case Description	Bulk Orders
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Bulk Service Order (SO) with all required data elements as described in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Service Order Confirmation (SOC) ○ Firm Order Commitment Notice (FOCN) ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A SO including at least 20 line items for services listed in Section C.2 of the contract ○ SO data provided via a delimited text file or MS Excel file

E.2.1.3.4.11 BSS-TS04-11: Error Checking: Missing Info

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-11
Test Case Description	Error Checking: Missing Information
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) missing one or more required data elements as described in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Service Order Rejection Notice (SORN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ SO missing one or more required data elements for one or more services listed in Section C.2 of the contract

E.2.1.3.4.12 BSS-TS04-12: Error Checking: Invalid Info

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-12
Test Case Description	Error Checking: Invalid Info
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) with one or more invalid data elements as described in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Service Order Rejection Notice (SORN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ SO orders with one or more invalid data information for one or more services listed in Section C.2 of the contract ○ Invalid data can include improperly formatted data or data that is inconsistent with the TO or Account Management data

E.2.1.3.5 BSS-TS05: Supplements to In-Progress Orders

E.2.1.3.5.1 BSS-TS05-01: Cancel Orders

Test Scenario	BSS-TS05: Supplements to In-Progress Orders
Test Case ID	BSS-TS05-01
Test Case Description	Cancel Orders
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 • Service Order (SO) for a cancellation of the previous order with all required data elements as described in Section J.2.4 issued prior to completion of the previous order
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Updates to Service Order Confirmation (SOC) if required ○ Updates to Firm Order Commitment Notice (FOCN) if required ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO for one or more services listed in Section C.2 of the contract ○ A second SO canceling the first Service Order as defined in Section J.2.10.1.1.4.3 ○ The Cancel Order may be issued before or after the deadline described in Section G.3

E.2.1.3.5.2 BSS-TS05-02: Service Feature Change

Test Scenario	BSS-TS05: Supplements to In-Progress Orders
Test Case ID	BSS-TS05-02
Test Case Description	Service Feature Change
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 • Service Order (SO) for a service feature change to the previous order with all required data elements as described in Section J.2.4 issued prior to completion to previous order
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Updates to Service Order Confirmation (SOC) if required ○ Updates to Firm Order Commitment Notice (FOCN) if required ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO for one or more services listed in Section C.2 of the contract ○ A second SO describing a service feature change to the first Service Order as defined in Section J.2.10.1.1.4.3

E.2.1.3.5.3 BSS-TS05-03: Location Change

Test Scenario	BSS-TS05: Supplements to In-Progress Orders
Test Case ID	BSS-TS05-03
Test Case Description	Location Change
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 • Service Order (SO) for a location change to the previous order with all required data elements as described in Section J.2.4 issued prior to completion to previous order
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Updates to Service Order Confirmation (SOC) if required ○ Updates to Firm Order Commitment Notice (FOCN) if required ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO for one or more services listed in Section C.2 of the contract ○ A second SO describing a location change to the first Service Order as defined in Section J.2.10.1.1.4.3

E.2.1.3.5.4 BSS-TS05-04: Change to Customer Want Date

Test Scenario	BSS-TS05: Supplements to In-Progress Orders
Test Case ID	BSS-TS05-04
Test Case Description	Change to Customer Want Date
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 • Service Order (SO) for a change to the Customer Want Date for the previous order with all required data elements as described in Section J.2.4 issued prior to completion of the previous order
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Updates to Service Order Confirmation (SOC) if required ○ Updates to Firm Order Commitment Notice (FOCN) if required ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO for one or more services listed in Section C.2 of the contract ○ A second SO describing a change to the Customer Want Date for the first Service Order as defined in Section J.2.10.1.1.4.3 ○ The Customer Want Date Change Order may be issued before or after the deadline described in Section G.3

E.2.1.3.5.5 BSS-TS05-05: Change to Administrative Data

Test Scenario	BSS-TS05: Supplements to In-Progress Orders
Test Case ID	BSS-TS05-05
Test Case Description	Change to Administrative Data
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.1.1.4.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 • Service Order (SO) for a change to the administrative data for the previous order with all required data elements as described in Section J.2.4 issued prior to completion of the previous order
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) ○ Updates to Service Order Confirmation (SOC) if required ○ Updates to Firm Order Commitment Notice (FOCN) if required ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO for one or more services listed in Section C.2 of the contract ○ A second SO describing a change to the administrative data for the first Service Order as defined in Section J.2.10.1.1.4.3

E.2.1.3.6 BSS-TS06: Administrative Change Orders

E.2.1.3.6.1 BSS-TS06-01: Administrative Change Order

Test Scenario	BSS-TS06: Administrative Change Order
Test Case ID	BSS-TS06-01
Test Case Description	Administrative Change Order
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS • One or more previously provisioned orders
Government Input(s)	• Administrative Change Order that specifies a change to the administrative data associated with a previously provisioned service as described in Section G.3
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Administrative Change (SOAC)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete administrative change order for a change to the administrative data for a previously provisioned service as described in Section G.3

E.2.1.3.7 BSS-TS07: Rapid Provisioning & Self-Provisioning Orders

E.2.1.3.7.1 BSS-TS07-01: Rapid Provisioning Orders

Test Scenario	BSS-TS07: Rapid Provisioning & Self-Provisioning Orders
Test Case ID	BSS-TS07-01
Test Case Description	Rapid Provisioning Orders
Requirements Reference(s)	• G.3 • G.5.3.1 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) for one or more services subject to rapid provisioning as defined in Section G.3 with all required data elements as described in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) if provisioning requires more than 24 hours ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ A complete SO for one or more services subject to rapid provisioning as defined in Section G.3

E.2.1.3.7.2 BSS-TS07-02: Self-Provisioning Orders

Test Scenario	BSS-TS07: Rapid Provisioning & Self-Provisioning Orders
Test Case ID	BSS-TS07-02
Test Case Description	Self-Provisioning Orders
Requirements Reference(s)	• G.3 • G.5.3.2 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) with all required data elements as described in Section J.2.4 for one or more services that are: ○ Subject to rapid provisioning as defined in Section G.3 ○ Available for self-provisioning as defined in Section G.3 and Section C.2
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4: ○ Service Order Acknowledgment (SOA) if provisioning requires more than 24 hours ○ Service Order Completion Notification (SOCN)
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ Service Order (SO) with all required data elements as described in Section J.2.4 for one or more services that are subject to rapid provisioning as defined in Section G.3 and that are available for self-provisioning as defined in Section G.3 and Section C.2

E.2.1.3.7.3 BSS-TS07-03: Self-Provisioning Orders: Error Checking

Test Scenario	BSS-TS07: Rapid Provisioning & Self-Provisioning Orders
Test Case ID	BSS-TS07-03
Test Case Description	Self-Provisioning Orders: Error Checking
Requirements Reference(s)	• G.3 • G.5.3.2 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
Government Input(s)	• Service Order (SO) for one or more services subject to rapid provisioning as defined in Section G.3 and available for self-provisioning • Populated via Contractors Portal with one or more missing or invalid data elements as described in Section J.2.4
Expected Output(s)	• Service Order notification CDRLs as defined in Section J.2.4 ○ Service Order Rejection Notice (SORN) ○ User is shown error message indicating failure
Acceptance Criteria	• All required CDRLs as defined in Section J.2.4 • Accurate data based on inputs • Correct technical aspects • Appropriate errors are displayed
Data Set Description	• Each government-provided test data set will include: ○ Service Order (SO) with all required data elements as described in Section J.2.4 for one or more services that are subject to rapid provisioning as defined in Section G.3 and that are available for self-provisioning as defined in Section G.3 and Section C.2 ○ SO to be provided via Contractors Portal

E.2.1.3.8 BSS-TS08: Inventory and Billing

E.2.1.3.8.1 BSS-TS08-01: Inventory Reconciliation

Test Scenario	BSS-TS08: Inventory and Billing
Test Case ID	BSS-TS08-01
Test Case Description	Inventory Reconciliation
Requirements Reference(s)	• G.7 • J.2.7
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS • One or more previously provisioned orders
Government Input(s)	• N/A
Expected Output(s)	• Inventory Reconciliation (IR) CDRLs as described in Section J.2.7
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• N/A, see Prerequisites

E.2.1.3.8.2 BSS-TS08-02: Billing

Test Scenario	BSS-TS08: Inventory and Billing
Test Case ID	BSS-TS08-02
Test Case Description	Billing
Requirements Reference(s)	• J.2.5 • J.2.10
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS • One or more previously provisioned orders
Government Input(s)	• N/A
Expected Output(s)	• Billing CDRLs as defined in Section J.2.4: ○ Billing Invoice (BI) ○ Tax Detail Report (TAX) ○ Associated Government Fee Detailed (AGFD) ○ AGF EFT Report (ATR)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects • CDRLs are internally consistent • Complies with calculation rules
Data Set Description	• N/A, see Prerequisites

E.2.1.3.8.3 BSS-TS08-03: Usage Based Billing

Test Scenario	BSS-TS08: Inventory and Billing
Test Case ID	BSS-TS08-03
Test Case Description	Usage Based Billing
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS • One or more previously usage based provisioned orders
Government Input(s)	• Sample usage data for one or more UBI based on Usage Based CLIN(s)
Expected Output(s)	• Billing CDRLs as defined in Section J.2.4: ○ Billing Invoice (BI) ○ Tax Detail Report (TAX) ○ Associated Government Fee Detailed (AGFD) ○ AGF EFT Report (ATR)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects • CDRLs are internally consistent • Complies with calculation rules
Data Set Description	• Each government-provided test data set will include: ○ Sample usage data for one or more UBI based on Usage Based CLIN(s) ○ See also Prerequisites

E.2.1.3.8.4 BSS-TS08-04: Billing Adjustments

Test Scenario	BSS-TS08: Inventory and Billing
Test Case ID	BSS-TS08-04
Test Case Description	Billing Adjustments
Requirements Reference(s)	• G.4 • J.2.5
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS • One or more previously provisioned orders • At least one previously submitted Billing Invoice (BI)
Government Input(s)	• Sample adjustment request to change or modify a billing line item
Expected Output(s)	• Billing Adjustment (BA) as defined in Section J.2.5: ○ Reflects requested adjustment
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ Sample adjustment request to change or modify a billing line item

E.2.1.3.9 BSS-TS09: Dispute Handling

E.2.1.3.9.1 BSS-TS09-01: Government Initiated Dispute

Test Scenario	BSS-TS09: Dispute Handling
Test Case ID	BSS-TS09-01
Test Case Description	Government Initiated Dispute
Requirements Reference(s)	• J.2.3 • J.2.6.3
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS • One or more previously provisioned orders • At least one previously submitted Billing Invoice (BI)
Government Input(s)	• Government issues at least 2 Disputes (D) as defined in Section J.2.6 • Notification to close a dispute after first Dispute Report is issued (see expected outputs)
Expected Output(s)	• Dispute Report (DR) ○ Reflects open Disputes • A second Dispute Report (DR) ○ Reflects open and closed Disputes
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Each government-provided test data set will include: ○ At least two Disputes (D) ○ Notification to close one or more disputes

E.2.1.3.10 BSS-TS10: SLA Management

E.2.1.3.10.1 BSS-TS10-01: SLA Reporting

Test Scenario	BSS-TS10: SLA Management
Test Case ID	BSS-TS10-01
Test Case Description	SLA Reporting
Requirements Reference(s)	• G.3 • J.2.4
Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS • One or more previously provisioned orders
Government Input(s)	• Services to show as SLAs met or missed
Expected Output(s)	• SLA Report (SLAR)
Acceptance Criteria	• All required CDRLs • Accurate data based on inputs • Correct technical aspects
Data Set Description	• Services by UBI to show as SLAs met or missed

E.2.1.3.10.2 BSS-TS10-02: SLA Credit Request

Test Scenario	BSS-TS10: SLA Management
Test Case ID	BSS-TS10-02
Test Case Description	SLA Credit Request
Requirements Reference(s)	• G.3 • J.2.4 • J.2.10.3.1.19

Prerequisites	• TO controlled, TO associated, and System Reference data loaded into contractor BSS
	  ○ One or more previously provisioned orders
	  ○ At least one previously submitted Billing Invoice (BI)
	  ○ SLA Report with at least one SLA missed

Government Input(s)	• SLA Credit Request (SLACR)
Expected Output(s)	• SLA Credit Request Response
Acceptance Criteria	• All required CDRLs • Each CDRL meets requirements
Data Set Description	• Each government-provided test data set will include: ○ SLA Credit Request

E.2.1.3.11 BSS-TS11: Open-Format Reporting

E.2.1.3.11.1 BSS-TS11-01: Open-Format Reporting: Samples

Test Scenario	BSS-TS11-01: Open-Format Reporting
Test Case ID	BSS-TS11-01
Test Case Description	Open-Format Reporting: Samples
Requirements Reference(s)	• G.4 • G.5 • J.2.10.2.1.13 • J.2.10.2.1.25 • J.2.10.2.1.26
Prerequisites	• N/A
Government Input(s)	• N/A

Expected Output(s)	• Sample copies of the contractor's standard reports for:
	  ○ Monthly Billing Information Memorandum
	  ○ Trouble Management Incident Performance Report
	  ▪ Describes service outage or degradation that are user initiated and/or automated monitoring created reports
	  ○ Trouble Management Performance Summary Report

Acceptance Criteria	• Each CDRL meets requirements
Data Set Description	• N/A

E.2.1.3.12 BSS-TS12: Regression Testing

E.2.1.3.12.1 BSS-TS12-01: Regression Testing

Test Scenario	BSS-TS12: Regression Testing
Test Case ID	BSS-TS12-01
Test Case Description	Regression Testing: Test Cases TBD
Requirements Reference(s)	• G.5.5
Prerequisites	• Contractor BSS has completed Development testing and ATO
Note	• Inputs, outputs, acceptance criteria and datasets to be determined based on Change Management provided in G.5.5 • Additional test cases may be defined as needed

E.2.1.3.13 BSS-TS13: Security Testing

E.2.1.3.13.1 BSS-TS13-01: Security Testing

Test Scenario	BSS-TS13: Security Testing
Test Case ID	BSS-TS13-01
Test Case Description	Security Testing
Requirements Reference(s)	• G.5.6
Prerequisites	• Defined in Section G.5.6 and references therein
Government Input(s)	• Defined in Section G.5.6 and references therein
Expected Output(s)	• Defined in Section G.5.6 and references therein
Acceptance Criteria	• Contractor BSS receives ATO
Data Set Description	• Defined in Section G.5.6 and references therein

E.2.1.4 Test Results

The contractor shall demonstrate that it successfully meets the BSS acceptance criteria for the various test scenarios/test cases defined in Sections E.2.1.2 and E.2.1.3. The Government will issue test results based on the deliverables for each test case. ~~The contractor shall provide test results that will provide details of testing the following:~~

~~Functional requirements for the Ordering, Billing, Inventory Management, Disputes, SLA Management and trouble ticketing processes as described in Section G and Section J.2.~~

~~System to system data exchange mechanism requirements defined in Section G.5 for each CDRLs defined in Section J.2.~~

~~Correct CDRLs are used in the data exchange.~~

~~Mandatory data elements for each CDRL defined in Section J.2.10 Data Dictionary are populated and accurate.~~

~~Available optional data elements for each CDRL defined in Section J.2.10 Data Dictionary are populated and accurate.~~

~~Timely and successful system to system data exchange to meet defined performance SLAs and provisioning intervals.~~

~~The test results shall detail at a minimum the following:~~

~~Test scenario # / Test case # / Test Data Set # / Test #; Date of Test performed, Acceptance Criteria, Test Result (Pass/Fail), etc.~~

E.2.1.5 Deliverables

E.2.1.5.1 Verification Test Plan for Contractor's BSS

The contractor shall submit a BSS Verification Test Plan (BSS Test Plan) based on the following timeline:

- Draft: with proposal
- Final: 30 days after NTP
- Revisions: 14 days after receipt of government comments

The BSS Test Plan shall:

- Reflect the test methodology defined in Section E.2.1.
- Include the contractor's approach to testing each test scenario and test case
- Include the contractor's timeline and test sequencing

E.2.2 EIS Services Verification Testing

The contractor shall provide an EIS Services Verification Test Plan (EIS Test Plan) based on the test methodology defined in this section(test scenarios, test cases, test data sets, acceptance criteria) in response to the RFP for each of the proposed EIS services.

E.2.2.1 General Testing Requirements

The contractor shall meet the following EIS Services testing requirements:

- Provide a verification and acceptance testing approach for all awarded EIS services defined in Section C.2.
- Develop an EIS Test Plan that includes, but is not limited to:
    - The test methodology for each EIS Service with test cases that will define the parameters to be measured, the measurement procedure, and the acceptance (pass/fail) criteria.
    - Fallback approach to describe the fallback process and procedures in case of testing failure.
    - An EIS Test Plan shall be required for all new services during the life of the contract.
    - Identification of any services from Section C.2 to which testing is not applicable.

The following conditions also apply:

- An agency may define additional testing in the TO.
- The contractor shall allow government representative(s) to observe all or any part of the EIS services verification testing.
- The contractor shall provide all necessary test equipment: data terminals, load boxes, test cables, and any other hardware and software required for testing.

E.2.2.2 Test Scenarios

The EIS Test Plan shall include, but not be limited to, the following test scenarios:

E.2.2.2.1 EIS Services Verification Test Scenarios

Test Scenario #	RFP Sec #	Description	Acceptance Criteria
Service TS-01	C.2	Demonstrate that the contractor's Cloud Services is compliant with Federal Risk and Authorization Management Program (FedRAMP) requirements as defined. • http://cloud.cio.gov http://cloud.cio.gov/fedramp/csp • NIST.gov publications http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_goodrich.pdf	The contractor shall provide FedRAMP certification and ensure that it is verified and accepted by GSA.
Service TS-02	G.8	Demonstrate that awarded services are delivered based on the KPIs and SLAs defined.	The contractor shall demonstrate that the service works properly according to KPIs defined in Section C.2.
Service TS-03	C.2.1.6.1.4	Verification Testing of Dark Fiber Services	See Section C.2.1.6.4 for acceptance criteria

E.2.2.3 Test Cases

The contractor shall provide test cases for each of the test scenarios defined in Section E.2.2.2. The test cases will be defined in the EIS Test Plan.

E.2.2.4 Test Data Sets

The contractor shall successfully test all of the test cases defined in the EIS Test Plan using one or more test data sets proposed by the contractor. The contractor shall test all services and service features proposed at the TO. The contractor shall use test data sets that reflect real-world service conditions and locations and shall address all relevant test cases.

E.2.2.5 Test Results and Acceptance

The contractor shall provide an EIS Services Verification Testing Report (EIS Testing Report) that shows successful completion of testing defined in the EIS Test Plan. The contractor shall complete verification and acceptance testing based on the acceptance criteria defined in the government accepted EIS Test Plan. Acceptance shall include government compliance requirements such as FedRAMP for cloud services, and the

ATO for FISMA related security requirements for EIS services. The contractor shall provide the following in order for the government to approve the test results:

- FedRAMP certification if cloud services are included in the TO.
- EIS Testing Report showing that each service provisioned works properly according to the KPIs defined in Section C.2 and the acceptance criteria defined in the EIS Test Plan.

Once verification testing is completed successfully the government may complete acceptance testing based on the acceptance criteria defined in the EIS Test Plan. The acceptance test will verify satisfactory end-to-end service performance and proper operation of all ordered features and functions. Performance will be considered satisfactory when services, equipment, systems and their associated features and functions perform as specified in the contract and TO. The contractor may not assign an effective billing date to an EIS Service until the agency accepts it in accordance with the agreed-upon acceptance testing procedures described in the EIS Test Plan.

The government reserves the right to perform additional tests to confirm proper operation of a delivered EIS service as defined by the TO. If the government does not report a problem to the contractor during this test period, the effective billing date will be the completion date on the SOCN. The contractor shall not begin billing for services if the government rejects the services within three (3) days of receipt of the SOCN. A longer period for test and acceptance may be specified in the TO. The contractor shall issue a new SOCN for services after correcting the reasons for rejection.

The service will be considered accepted if the government does not reject the service within the acceptance period defined above. If the government rejects the service, it may at its option:

1. Direct the contractor to repeat the procedure outlined above;
2. Withdraw the service from acceptance testing;
3. Direct the contractor to facilitate the return of the services to their original provider (for services transitioned or migrated from another contractor's network);
4. Request a replacement of the service (in whole or in part); or
5. Cancel the service order without penalty.

If the government exercises any of these options as a consequence of unacceptable acceptance testing results, all expenses incurred by the government shall be borne by the contractor.

If the government elects option 1 above, the contractor shall immediately initiate corrective actions to remedy the problem reported on the trouble ticket and shall keep

the government informed of progress. In such cases, the government reserves the right to exercise option 2, 3, 4 or 5 at any time.

If the government elects any of the options above other than option 1, all expenses incurred by the government, including recurring charges and non-recurring charges (NRC) to return services to the previous network configuration, shall be borne by the contractor. In cases when the government cannot successfully complete acceptance testing due to circumstances beyond the control of the contractor, the contractor shall notify government of the details surrounding the deficiencies and the steps the contractor has taken to overcome the deficiencies.

These cases shall be discussed between the government and the contractor. On a case-by-case basis, the GSA CO or the OCO may choose to waive the acceptance testing or extend the testing period. Waiver of the acceptance testing may be considered in those instances when the contractor has demonstrated that the problems encountered are not the fault of the contractor and government has determined that the contractor has taken all reasonable actions to correct all problems. The waiver issued by the GSA CO or the OCO will specify the grounds for the waiver. If the waiver is not granted, the contractor shall be obligated to continue to attempt correction of the deficiencies encountered in order to successfully accomplish the acceptance testing.

E.2.2.6 Deliverables

The contractor shall provide an EIS Test Plan in its proposal that describes the testing of EIS Services based on test methodology described in Sections E.2.2.1 – E.2.2.5. Updates shall be submitted for any new services that are added to the contract with the modification proposal.

The contractor shall provide an EIS Testing Report as defined in Section E.2.2.5 within 3 days of service installation and testing.

Enterprise Infrastructure Solutions (EIS)
Contract

Section F
Deliveries or Performance

Issued by:

General Services Administration

Office of Information Technology Category

[redacted]

~~November 2017~~January 2019

Table of Contents

F.1 FAR 52.252-2 Clauses Incorporated by Reference (FEB 1998)

This contract incorporates one or more FAR clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer (CO) will make their full text available. The full text of a clause may be accessed electronically at this address: www.acquisition.gov/far.

The clauses below apply at the contract and order levels, as applicable, depending upon the contract type of the order, or as specifically referenced in the applicable order.

Clause No.	FAR Clause No.	Title and Date
F.1.1	52.242-15	Stop Work Order (AUG 1989)
F.1.2	52.242-17	Government Delay of Work (APR 1984)
F.1.3	52.247-35	F.O.B. Destination Within Consignee's Premises (APR 1984)

F.2 Deliverables

The contractor shall ensure that all deliverables meet professional standards and the requirements set forth in the contract. The contractor shall be responsible for delivering all items (as required) in accordance with the Table of Deliverables below:

F.2.1 Table of Deliverables

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
1.	B.1.1	B.1.1	Task Order Pricing Tables	Initial: Included at task order (TO) award Update: As needed	GSA Systems and agency
2.	B.1.2.9	B.1.2.9	Price Volume	Initial: With the proposal Update: As needed	GSA Systems
3.	B.1.3	B.1.3	Online Catalog	Initial: Within 30 days of contract award Update: As needed	Website – URL to be provided by contractor
4.	B.1.3	B.1.3	Catalog Pricing Tables (Section B)	Initial: Included at TO award Update: As needed	GSA Systems and agency
5.	C.2.8.4.5.4	NIST SP 800-53 R4; PL-2	System Security Plan (SSP)	Initial: Within 30 days of Notice to Proceed (NTP) Update: Annually from contract award and when significant changes occur	GSA COR/ISSO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
6.	C.2.8.4.5.4	NIST SP 800-37 R1	Security Assessment Boundary and Scope Document (BSD)	Initial: Within 15 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
7.	C.2.8.4.5.4	NIST SP 800-53 R4; CA-3	Information System Interconnection Security Agreements (ISA)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
8.	C.2.8.4.5.4	NIST SP 800-53 R4; AC-1	GSA NIST 800-53 R4 Control Tailoring Workbook	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
9.	C.2.8.4.5.4	NIST SP 800-53 R4; AC-1	GSA NIST SP 800-53 R4 Control Summary Table	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
10.	C.2.8.4.5.4	NIST SP 800-53 R4; PL-4	Rules of Behavior (RoB)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
11.	C.2.8.4.5.4	NIST SP 800-53 R4; CM-8	System Inventory	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
12.	C.2.8.4.5.4	NIST SP 800-53 R4; CP-2	Contingency Plan (CP)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
13.	C.2.8.4.5.4	NIST SP 800-53 R4; CP-4	Contingency Plan Test Plan (CPTP)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
14.	C.2.8.4.5.4	NIST SP 800-53 R4; CP-4	Contingency Plan Test Report (CPTR)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
15.	C.2.8.4.5.4	NIST SP 800-53 R4; AR-2, AR-3 and AR-4	'Privacy Threshold Assessment (PTA)/Privacy Impact Analysis (PIA)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
16.	C.2.8.4.5.4	NIST SP 800-53 R4; CM-9	Configuration Management Plan (CMP)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
17.	C.2.8.4.5.4	NIST SP 800-53 R4; IR-8	Incident Response Plan (IRP)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
18.	C.2.8.4.5.4	NIST SP 800-53 R4; IR-3	Incident Response Test Report (IPTR)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
19.	C.2.8.4.5.4	NIST SP 800-53 R4; SA-12 and NIST SP 800-161	Supply Chain Risk Management Plan (SCRM)	Initial: With the proposal Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
20.	Reserved	Reserved	Reserved	Reserved	Reserved
21.	C.2.8.4.5.4	NIST SP 800-53 R4; CA-5	Plan of Action and Milestones (POA&M)	Initial: With the Security A&A package Update: Quarterly Note: Critical and High vulnerabilities shall be updated monthly	GSA COR/ISSO
22.	C.2.8.4.5.4	NIST SP 800-53 R4; CA-7 and RA-5	Independent internal and external penetration tests and reports	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
23.	C.2.8.4.5.4	NIST SP 800-53 R4; SA-11	Code Review Report (If applicable)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
24.	C.2.8.4.5.4	NIST SP 800-53 R4; CA-2	Annual FISMA Assessment	Annually on the first day of August and when significant changes occur	GSA COR/ISSO
25.	C.2.8.4.5.4	NIST SP 800-53 R4; CM-6	SCAP Common Configuration Enumerations (CCE) Report	Initial: With the Security A&A package Update: Monthly (end of month)	GSA COR/ISSO
26.	C.2.8.4.5.4	NIST SP 800-53 R4; CM-8	SCAP Common Platform Enumeration (CPE) Report	Initial: With the Security A&A package Update: Monthly (end of month)	GSA COR/ISSO
27.	C.2.8.4.5.4	NIST SP 800-53 R4; CM-8	SCAP Common Vulnerabilities and Exposures (CVE)	Initial: With the Security A&A package Update: Monthly (end of month)	GSA COR/ISSO
28.	C.2.9.1.1	C.2.9.1.1	Site Survey Report	As needed	OCO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
29.	C.3.3.3	C.3.3.3	Inventory Summary of All Active Services	Initial: 3 years prior to contract expiration Update: As requested by GSA	GSA Transition Manager
30.	C.3.3.3	C.3.3.3	Inventory Summary of Agency's Active Services	Initial: 3 years prior to contract expiration Update: As requested by agency	OCO
31.	C.3.3.4	C.3.3.4	Transition Inventory Report	Initial: 3 years prior to contract expiration Update: Weekly (end of week)	GSA Transition Manager
32.	C.3.3.4	C.3.3.4	Transition Status Report	Initial: 3 years prior to contract expiration Update: Monthly (end of month)	GSA Transition Manager
33.	C.4.2	C.4.2	Voluntary Product Accessibility Template	Initial: 30 days after NTP Update: As needed	Contractor's public website
34.	E.2.1.5.1	E.2.1.5.1	BSS Verification Test Plan	Draft: With proposal Update: Final 30 days after NTP; others within 14 days of government request	GSA CO
35.	Reserved	Reserved	Reserved	Reserved	Reserved
36.	E.2.2.6	E.2.2.6	EIS Services Verification Test Plan	Initial: With proposal Update: As needed	GSA COR
37.	G.3.2.3.1	G.3.2.3.1	Fair Opportunity Notice of Protest	Initial: Within three business days of protest Update: As needed	GSA CO
38.	G.3.3.3.3	G.3.3.3.3	Task Order Project Plan	Initial: TO award Update: Plan change	OCO
39.	G.5.5	G.5.5	BSS Development & Implementation Plan	Initial: With proposal Update: Plan change	GSA CO
40.	G.5.5.1	G.5.5.1	BSS Change Control Notification	30 days prior to BSS changes or emergency changes	GSA COR/ISSO/ISSM
41.	G.5.6.4	NIST SP 800-53 R4; CA-5 NIST SP 800-53 R4; RA-5	Plan of Action and Milestones (POA&M) Vulnerability scanning reports for Operating System, Web Application, and Database scans (as applicable)	Initial: With the Security A&A package Update: Quarterly	GSA COR/ISSO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
42.	G.5.6.4	NIST SP 800-53 R4; PL-2	BSS System Security Plan (SSP)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
43.	G.5.6.4	NIST SP 800-37 R1	Security Assessment Boundary and Scope Document (BSD)	Initial: Within 15 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
44.	G.5.6.4	NIST SP 800-53 R4; CA-3	Information System Interconnection Security Agreements (ISA)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
45.	G.5.6.4	NIST SP 800-53 R4; AC-1	GSA NIST 800-53 R4 Control Tailoring Workbook	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
46.	G.5.6.4	NIST SP 800-53 R4; AC-1	GSA NIST SP 800-53 R4 Control Summary Table	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
47.	G.5.6.4	NIST SP 800-53 R4; PL-4	Rules of Behavior (RoB)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur.	GSA COR/ISSO
48.	G.5.6.4	NIST SP 800-53 R4; CM-8	System Inventory	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
49.	G.5.6.4	NIST SP 800-53 R4; CP-2	Contingency Plan (CP)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
50.	G.5.6.4	NIST SP 800-53 R4; CP-4	Contingency Plan Test Plan (CPTP)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
51.	G.5.6.4	NIST SP 800-53 R4; CP-4	Contingency Plan Test Report (CPTR)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
52.	G.5.6.4	NIST SP 800-53 R4; AR-2, AR-3 and AR-4	'Privacy Threshold Assessment (PTA)/Privacy Impact Analysis (PIA)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
53.	G.5.6.4	NIST SP 800-53 R4; CM-9	Configuration Management Plan (CMP)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
54.	G.5.6.4	NIST SP 800-53 R4; IR-8	Incident Response Plan (IRP)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
55.	G.5.6.4	NIST SP 800-53 R4; IR-3	Incident Response Test Report (IRTR)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
56.	Reserved	Reserved	Reserved	Reserved	Reserved
57.	G.5.6.4	NIST SP 800-53 R4; CA-7 and RA-5	Independent internal and external penetration tests and reports	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
58.	G.5.6.4	NIST SP 800-53 R4; SA-11	Code Review Report (If applicable)	Initial: Prior to placing the information system into production Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
59.	G.5.6.4	NIST SP 800-53 R4; CA-2	Annual FISMA Assessment	'Annually on the first day of August and when significant changes occur	GSA COR/ISSO
60.	G.5.6.4	NIST SP 800-53 R4; AC-1	Access Control Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
61.	G.5.6.4	NIST SP 800-53 R4; AT-1	Security Awareness and Training Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
62.	G.5.6.4	NIST SP 800-53 R4; AU-1	Audit and Accountability Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
63.	G.5.6.4	NIST SP 800-53 R4; CA-1	Security Assessment and Authorization Policies and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
64.	G.5.6.4	NIST SP 800-53 R4; CM-1	Configuration and Management Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
65.	G.5.6.4	NIST SP 800-53 R4; CP-1	Contingency Planning Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
66.	G.5.6.4	NIST SP 800-53 R4; IA-1	Identification and Authentication Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
67.	G.5.6.4	NIST SP 800-53 R4; IR-1	Incident Response Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
68.	G.5.6.4	NIST SP 800-53 R4; MA-1	System Maintenance Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
69.	G.5.6.4	NIST SP 800-53 R4; MP-1	Media Protection Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
70.	G.5.6.4	NIST SP 800-53 R4; PE-1	Physical and Environmental Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
71.	G.5.6.4	NIST SP 800-53 R4; PL-1	Security Planning Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
72.	G.5.6.4	NIST SP 800-53 R4; PS-1	Personnel Security Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
73.	G.5.6.4	NIST SP 800-53 R4; RA-1	Risk Assessment Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
74.	G.5.6.4	NIST SP 800-53 R4; SA-1	Systems and Services Acquisition Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
75.	G.5.6.4	NIST SP 800-53 R4; SC-1	System and Communication Protection Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
76.	G.5.6.4	NIST SP 800-53 R4; SI-1	System and Information Integrity Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
77.	G.6.3.1	G.6.3.1	Supply Chain Risk Management (SCRM) Plan	Initial: With proposal Update: Annually from contract award	CO/COR
78.	G.9.3	G.9.3	Contractor Points of Contact List	Initial: 30 days after NTP Update: As needed	Contractor's public website
79.	G.9.4	G.9.4	Program Management Plan (PMP)	Initial: With proposal Update: As needed	GSA CO
80.	G.9.5	G.9.5	Financial Status Report	Initial: 30 days after NTP; Update: 15th of each subsequent month	GSA PMO
81.	G.9.6.1	G.9.6.1	Quarterly Program Status Reports	Initial: 90 days after NTP Update: Quarterly (One business day prior to each Quarterly Meeting)	GSA CO
82.	G.10	G.10	Customer Training Plan	Draft: With proposal Update: 15 days after government review	GSA COR
83.	G.11	G.11	NS/EP Functional Requirements Implementation Plan	Initial: With proposal Update: Annually from contract award	GSA COR
84.	G.12.1	G.12.1	Corporate Climate Risk Management Plans	Initial: With proposal Update: As needed	GSA CO, OCO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
85.	G.12.2.1	G.12.2.1	Climate Change Adaptation, Sustainability, and Green Initiatives Report	Initial: By award Update: Annually from contract award	GSA CO, GSA COR, OCO
86.	G.12.2.3	G.12.2.3	Power Utilization Efficiencies (PUE) Report	Initial: Task Order from Proposal Update: Annually	OCO
87.	H.7.3	H.7.3	Three Largest Comparable Multi-Service Contracts per Service	30 days after request	GSA COR
88.	H.7.3	H.7.3	Three Largest Comparable Single-Service Contracts per Service	30 days after request	GSA COR
89.	H.9	H.9	Redacted Contract	Initial: 30 days after award Update: Post - No later than the 12th day of each month to reflect all contract mods from previous month Provide: to GSA CO no later than 7 days	Contractor's public website (for posting redacted contract and mods); GSA CO (if requested)
90.	H.10.2	H.10.2	Key Personnel	Initial: With proposal Update: Within 15 days of change or 30 days if clearance to be obtained	GSA CO
91.	H.10.3	H.10.3	Organizational Structure	Initial: With proposal Update: Within 30 calendar days of change	GSA CO
92.	H.14	H.14	State and Local Taxes	Report semi-annually from the date of the NTP. Request to add new taxes 30 days prior to inclusion on an invoice	GSA CO
93.	H.23	H.23	Fees and Surcharges	Report semi-annually from the date of the NTP. Request to add new fees and surcharges 30 days prior to inclusion on an invoice	GSA CO
94.	H.25	H.25	Service Trials Notification	Prior to initiation of any trial program with the agency	GSA CO and OCO
95.	H.25	H.25	Service Trial Status Report	Monthly (first business day) until completion of each trial	OCO
96.	H.33	H.33	ESI requests/searches	Within 15 days of written request	GSA CO or OCO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
97.	H.34	H.34	Tariff Filings	Initial: Within 60 days of NTP Update: New and/or revisions to existing tariffs at least 10 days in advance of intended filing date	GSA CO
98.	H.36	H.36	Monitoring Information and eSRS Reporting	Monitoring information and eSRS reporting April 30 and October 30 each year after NTP	GSA CO
99.	H.38	H.38	Force Majeure Notification	Within 10 days of the cause that the contractor cites for Force Majeure	OCO
100.	J.2.3	J.2.3.2 J.2.10.2.3.1	TO CLINs Awarded	Initial: At TO award Update: As required	GSA Systems
101.	J.2.3	J.2.3.2 J.2.10.2.3.4	TO Jurisdictions Awarded by Service	Initial: At TO award Update: As required	GSA Systems
102.	J.2.3	J.2.3.2 J.2.10.2.3.7	TO Officials	Initial: At TO award Update: As required	GSA Systems
103.	J.2.3	J.2.3.2 J.2.10.2.3.2	TO Customer Requirements Document Set	Initial: At TO award Update: As required	GSA Systems
104.	J.2.3	J.2.3.2 J.2.10.2.3.3	TO Financials	Initial: At TO award Update: As required	GSA Systems
105.	J.2.3	J.2.3.2 J.2.10.2.3.5	TO Key Performance Indicators	Initial: At TO award Update: As required	GSA Systems
106.	J.2.3	J.2.3.2 J.2.10.2.3.6	TO Locations Awarded by Service	Initial: At TO award Update: As required	GSA Systems
107.	J.2.3	J.2.3.2 J.2.10.2.3.8	TO Service Awarded	Initial: At TO award Update: As required	GSA Systems
108.	J.2.3	J.2.3.2 J.2.10.2.1.8	Direct Billed Agency Setup (DBAS)	Initial: At TO award Update: As required	GSA Conexus
109.	Reserved	Reserved	Reserved	Reserved	Reserved
110.	J.2.4	J.2.4.2 J.2.10.2.1.16	Service Order Acknowledgement (SOA)	NLT one (1) business day after Service Order (SO)	GSA Conexus and agency COR
111.	J.2.4	J.2.4.2 J.2.10.2.1.20	Service Order Rejection Notice (SORN)	NLT 5 days after SO	GSA Conexus and agency COR
112.	J.2.4	J.2.4.2 J.2.10.2.1.19	Service Order Confirmation (SOC)	NLT 5 days after SO	GSA Conexus and agency COR

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
113.	J.2.4	J.2.4.2 J.2.10.2.1.11	Firm Order Commitment Notice (FOCN)	Local access subcontractor required: • Within one (1) business day of receiving FOC date Local access subcontractor not required: NLT the earlier of: • 5 days after SOC, or • 10 days before the FOC date	GSA Conexus and agency COR
114.	J.2.4	J.2.4.2 J.2.10.2.1.18	Service Order Completion Notice (SOCN)	NLT 3 days after service is installed and tested	GSA Conexus and agency COR
115.	J.2.4	J.2.4.2 J.2.10.2.1.17	Service Order Administrative Change (SOAC)	NLT 7 days after Administrative Change Order	GSA Conexus and agency COR
116.	J.2.4	J.2.4.2 J.2.10.2.1.21	Service State Change Notice (SSCN)	Cloud Services: • Within 24 hours of state change. All other services: • NLT 5 business days prior to submission of associated BI	GSA Conexus and agency COR
117.	J.2.5	J.2.5.2 J.2.10.2.1.5	Billing Invoice (BI)	Monthly, NLT 15th business day	GSA Conexus and agency COR
118.	J.2.5	J.2.5.2 J.2.10.2.1.24	Tax Detail	Monthly, NLT 15th business day	GSA Conexus and agency COR
119.	J.2.5	J.2.5.2 J.2.10.2.1.2	AGF Detail	Monthly, NLT 15th business day	GSA Conexus
120.	J.2.5	J.2.5.2 J.2.10.2.1.3	AGF Electronic Funds Transfer Report (ATR)	Monthly, NLT 15th business day	GSA Conexus
121.	J.2.5	J.2.5.2 J.2.10.2.1.13	Monthly Billing Information Memorandum	Monthly, NLT 15th business day (as needed)	Agency COR
122.	J.2.5 J.2.6 J.2.8	J.2.5.2 J.2.6.2 J.2.8.2 J.2.10.2.1.4	Billing Adjustment (BA)	Monthly, NLT 15th business day (as needed)	GSA Conexus and agency COR
123.	Reserved	Reserved	Reserved	Reserved	Reserved
124.	J.2.6	J.2.6.2 J.2.10.2.1.10	Dispute Report (DR)	Monthly, NLT 15th business day (as needed)	GSA Conexus and agency COR
125.	J.2.7	J.2.7.2 J.2.10.2.1.12	Inventory Reconciliation	Monthly, NLT 15th day of month	GSA Conexus

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
126.	J.2.8	J.2.8.2 J.2.10.2.1.14	Service Level Agreement Report (SLAR)	Monthly, NLT 15th day of month	GSA Conexus, OCO and agency COR
127.	J.2.8	J.2.8.2 J.2.10.2.1.22	SLA Credit Request Response	Within 30 days of SLA Credit Request	OCO and agency COR
128.	J.2.8	J.2.8.2 J.2.10.2.1.25	Trouble Management Performance Summary Report	Quarterly, NLT 15 days after the end of the FY quarter	Agency COR
129.	J.2.8	J.2.8.2 J.2.10.2.1.24	Trouble Management Incident Performance Report	Quarterly, NLT 15 days after the end of the FY quarter	Agency COR
130.	J.2.10.3.1.2	J.2.10.3.1.2, row for adjustment aggregated_tax	Adjustment Aggregated Tax AGF Inclusion Notice	Initial to GSA: NLT ATO Initial to Agency: At TO award Updates to GSA and Agency: Upon approval of associated BSS change (See Section G.5.5.1)	GSA CO, GSA COR, OCO and agency COR

Enterprise Infrastructure Solutions (EIS) Contract

Section G
Contract Administration Data

Issued by:

General Services Administration

Office of Information Technology Category

[redacted]

~~May 2018~~January 2019

Table of Contents

G.1 Introduction

This section provides management and operational requirements for the Enterprise Infrastructure Solutions (EIS) contract. The functional areas covered include:

- Contract Administration
- Ordering
- Billing
- Business Support Systems
- Service Assurance
- Inventory Management
- Service Level Management
- Program Management
- Training
- National Security and Emergency Preparedness
- Requirements for Climate Change Adaptation, Sustainability and Green Initiatives

Additional requirements associated with this section related to data interchange, including deliverables and the data dictionary, are further defined in Section J.2 Contractor Data Interaction Plan.

For the purposes of this contract, all days are CALENDAR days unless otherwise specified.

G.2 Contract Administration

G.2.1 Government Points of Contact

The administration of this contract will require coordination between the government and the contractor. The following sections describe the roles and responsibilities of individuals who will be the points of contact for the government and the contractor on matters concerning contract administration.

G.2.2 Roles and Responsibilities

G.2.2.1 Agency Role

With regard to task orders (TOs), service orders and billing for services, agencies are responsible for:

1. Placing TOs according to FAR Subpart 16.505, and service orders in accordance with the terms and conditions of the contract.
2. Accepting or rejecting the services rendered by the contractor under TOs and service orders in accordance with Section E.2.2 EIS Services Verification Testing, and coordinating corrective actions with the contractor and GSA if required.
3. Coordinating resources and service providers to facilitate scheduling and communications for implementing and maintaining service. This includes:
    a) Identifying the agency's Local Government Contacts (LGCs) for each location involved in a particular project or other TO or service order activity, if possible.
    b) Monitoring and facilitating coordination between the contractor and LGC and other agency vendors and service providers as appropriate.
    c) Coordinating with users, and with other contractor(s) that are providing the location with telephone switching or other telecommunications facilities, upon notification by the contractor of changes regarding the date of scheduled activities or site requirements.
4. Paying the contractor for services provided.
5. Notifying the contractor of billing errors and facilitating the resolution thereof.
6. Additional roles and responsibilities contained in any Delegation of Procurement Authority (DPA) issued by a GSA Contracting Officer (GSA CO) to a warranted agency Ordering Contracting Officer or authorized official.
7. Additional roles and responsibilities contained in any Contracting Officer's Representative (COR) Designation Letter.

G.2.2.1.1 Task Order Authority / OCO

As described in Section G.3 Ordering, only a warranted contracting officer or other authorized official with authority to obligate funds for the agency (or tribe, or other entity authorized to use the contract per OGP 4800.2I) and who has been granted DPA by a GSA CO may issue or modify a TO under the contract. The contractor shall ensure that an OCO or an authorized official (hereinafter referred to as "OCO") has the required DPA prior to processing TOs; this information will be available to the contractor in GSA Systems.

G.2.2.1.2 OCO Duties

The OCO duties include, but are not limited to, those specified in the DPA in Attachment J.3 Delegation of Procurement Authority. The OCO for each TO may designate COR(s) authorized to place service orders specified in the TO.

Appointment and Training: The COR is a federal employee with Federal Acquisition Certification – Contracting Officer's Representative (FAC-COR) certification and complete contractor-provided training related to placement of service orders. If the agency does not use the FAC-COR certification process, the OCO may appoint an individual who is responsible for these duties. The COR will be delegated limited TO contract administration authority through a COR appointment letter by the OCO with DPA.

The COR duties may include, but are not limited to, the following tasks:

1. Understanding the contractor's service order procedures and being fully aware of the requirements and limits delegated by the OCO.
2. Placing service orders under a TO using the appropriate billing codes.
3. Accepting services ordered and verifying that services meet technical requirements.
4. Confirming funding availability prior to service ordering.
5. Coordinating with the appropriate budget and finance offices and the OCO to execute processes and internal controls to support funding availability and to comply with the Antideficiency Act (31. U.S.C 1341) and/or other applicable laws regarding funding.
6. Executing other duties related to ordering (e.g., billing disputes), as defined by the OCO.

G.2.2.2 GSA Role

GSA's primary role is contract administration. GSA is responsible for administering this contract and will modify the contract as necessary. In addition, GSA will:

1. Ensure compliance with contract requirements.
2. Delegate procurement authority to agencies to authorize OCOs to place TOs.
3. Place TOs on the agency's behalf, if so requested.
4. Assist in resolving conflicts between the contractor and the agency if necessary.

G.2.2.2.1 GSA Contracting Officer

The GSA CO has overall responsibility for administering the contract. The right to issue contract modifications, change the terms and conditions of the contract, terminate the contract, exercise option renewals, and approve subcontractors is reserved solely for the GSA CO unless otherwise delegated in writing. The GSA CO will be identified upon award.

G.2.2.2.2 GSA Program Manager

The GSA Program Manager will provide central technical oversight and management regarding this contract to the contractor, GSA, and agency customers.

G.2.2.2.3 GSA Contracting Officer's Representative (COR)

A GSA COR will be designated by the GSA CO to monitor certain technical aspects of the contract. Actions within the purview of the GSA COR's authority include:

1. Ensuring that the contractor performs the technical requirements of the contract.
2. Performing or directing the inspections necessary to verify and validate service delivery specified under the contract.
3. Monitoring the contractor's performance under the contract, including SLA compliance, and notifying the contractor and the CO of any deficiencies observed.

A letter of delegation will be issued by the GSA CO to the GSA COR, with a copy supplied to the contractor, stating the COR's responsibilities and limitations.

The COR's authority does not include the ability to authorize work not already in the contract or to modify the terms and conditions of the contract.

G.2.2.2.4 GSA Customer Service Representative

The customer service representative for GSA is the Technology Service Manager (TSM), who works with agencies to inform them of contractor service offerings. The

TSM's authority does not include the ability to authorize work not already in the contract or to modify the terms and conditions of the contract. The TSM assigned to an agency account provides customer support to ensure the agency's satisfaction with delivery, operation, maintenance, and billing of services.

G.2.2.2.5 Delegation of Procurement Authority

GSA establishes a DPA from the GSA CO to the OCO, and complies with the Office of Management and Budget's (OMB) Executive Agent designation to GSA. See Section J.3.

G.2.3 BSS Final Contract Acceptance

The contractor shall complete and pass the BSS validation testing, as stated in the contract, within 12 months from the acceptance of the BSS Verification Test Plan (see Section E.2.1). For the purposes of this section (G.2.3), BSS validation testing does not include completion of Assessment and Authorization (A&A) as referenced in Section E.2.1.2.2, Test Scenario BSS-TS13. If the contractor does not pass the BSS testing in the 12-month period, the government shall cancel the contract; however, the contractor will receive additional time due to delays caused by the government. The contractor shall not receive the Minimum Revenue Guarantee (MRG) stated in Clause H.3 if its contract is cancelled in accordance with this clause. The government shall not entertain any financial claim or settlement submitted by the contractor as a result of the contract being cancelled.

G.2.4 Contract Modification

A contract modification may be requested by GSA, the contractor, or an agency as described in Section J.4 Guidelines for Modifications to EIS Program Contracts.

G.2.5 Contract Closeout

Contract closeout will be accomplished within the guidelines set forth in:

- FAR Part 4.804 Closeout of Contract Files
- GSAM Subpart 504.804-5 Procedures for closing out contract files

G.2.6 Past Performance

In accordance with FAR 42.15 Contractor Performance Information, and individual agency policy, the OCO will prepare an evaluation of the contractor's performance for each TO that exceeds the simplified acquisition threshold of $~~1~~250,000 using the Contractor Performance Assessment Reporting System (CPARS). CPARS allows the contractor to view and comment on the government's evaluation of the contractor's

performance before it is finalized. Once the contractor's past performance evaluation is finalized in CPARS, it will be transmitted into the Past Performance Information Retrieval System (PPIRS) at http://www.ppirs.gov/.

G.3 Ordering

This section applies to all orders (services, equipment, and labor) under the contract. The contractor may only accept orders from entities listed in OGP 4800.2I Eligibility to use GSA Sources of Supply and Services.

The following steps are a high-level summary of the ordering process:

1. GSA establishes a DPA from the GSA CO to the OCO.
2. The OCO completes the fair opportunity process.
3. The OCO issues a TO that complies with FAR 16.505.
4. The OCO may appoint a COR(s) or other authorized ordering official on the TO to assist with the administration and placing of service orders.
5. Once the TO is awarded, the OCO completes account registration with the contractor.
6. Government may place service orders against the TO.

G.3.1 Fair Opportunity Process

Fair opportunity will be accomplished through an RFQ (Request for Quotation) or RFP (Request for Proposal). The RFQ/RFP can be as complex as an entire agency network or as simple as a comparison of existing priced CLINs.

The OCO will follow the fair opportunity procedures and exceptions specified in FAR 16.505, including but not limited to the following:

1. The OCO must provide each awardee a fair opportunity to be considered for each TO exceeding $3,500 unless one of the exceptions in FAR 16.505(b)(2) applies.
2. For fair opportunity for TOs from $3.5K - $~~1~~2250K, the OCO must provide each awardee a fair opportunity to be considered for each TO. If the order does not exceed the simplified acquisition threshold, the OCO need not contact each of the multiple awardees under the contract before selecting a TO awardee if the OCO has information available to ensure that each awardee is provided a fair opportunity to be considered for each TO.
3. For fair opportunity for TOs exceeding the simplified acquisition threshold (more than $~~1~~2250K and less than $5.5M), each TO shall be placed on a competitive basis in accordance with the following.
    a) Provide a fair notice of the intent to make a purchase, including a clear description of the supplies to be delivered or the services to be performed and

the basis upon which the selection will be made to all contractors offering the required supplies or services under the contract.

b) Afford all contractors responding to the notice a fair opportunity to submit an offer and have that offer fairly considered.

4. For fair opportunity for TOs exceeding $5.5 million, the contracting officer shall provide at a minimum:

   a) A notice of the TO that includes a clear statement of the agency's requirements.

   b) A reasonable response period (as defined by the OCO on the TO).

   c) Disclosure of the significant factors and sub-factors the agency expects to consider in evaluating proposals, including cost or price, and their relative importance.

   d) If award is made on a best value basis, a written statement documenting the basis for award and the relative importance of quality and cost or price.

   e) An opportunity for a post-award debriefing.

The OCO will include the evaluation procedures in the RFQ/RFP and establish the timeframe for responding, giving the contractor a reasonable proposal preparation time while taking into account any unique requirements and circumstances. All costs associated with the preparation, presentation, and discussion of the contractor's proposal in response will be at the contractor's sole and exclusive expense.

G.3.1.1 eBuy

The government may issue solicitations via GSA's eBuy (https://www.ebuy.gsa.gov). EBuy is an online RFQ/RFP tool designed to facilitate offerings for a wide range of supplies and services. EBuy allows the government to post requirements and obtain quotes/proposals. Posting on eBuy satisfies all requirements for providing fair opportunity notice to potential offerors, even if fewer than three offers are received. Use of the eBuy system fulfills the notification requirements in FAR 16.505.

Registration in eBuy is required to view and respond to solicitations in eBuy. After registration, the contractor is strongly encouraged to monitor eBuy frequently for opportunities. Industry partners will receive notices regarding opportunities in eBuy at their registered e-mail addresses. Contractors shall respond in the manner prescribed in the request. To respond to opportunities in eBuy, use https://www.ebuy.gsa.gov.

G.3.2 Task Orders

TOs will identify the services required and will provide specific technical details and scope of work required, including the schedule for all deliverables and the identification of any applicable equipment and labor categories, and service level performance. A TO

will still be required for low-value orders that are under the fair opportunity threshold (see Section G.3.1)~~, unless the order is funded entirely via a government purchase card (see Section G.4.8)~~.

TOs may contain a combination of priced CLINs, Task Order Unique CLINs (TUCs), and Individual Case Basis (ICB) CLINs depending on agency-specific requirements for services, features, and performance. Agencies may require services that, although within the scope of the contract, are not available to order with priced CLINs.

TUCs are defined in Section B.1.2.2 and may be used to assist in defining special requirements for ordering and billing purposes or to combine multiple CLINs under a single overarching CLIN. TUC pricing submission details are described in Section J.4.1.

ICB CLINs are defined in Section B.1.2.14 and may be used to provide unique identifiers for services that are yet to be fully defined for a particular service under a specific TO. ICB CLINs are defined for various services on the contract (e.g., an OC-12 Access Arrangement) but require additional information to determine the price for the individual case and TO.

For each TO, the OCO is the sole and exclusive government official with authority to take actions that may bind the government. The OCO will have a DPA issued by GSA (see G.2.2.1.1 for the contractor's responsibilities regarding the DPA). The OCO may designate a COR or authorized ordering official to assist the OCO with administering the TO. The contractor shall not accept or bill the government for TOs or service orders from an unauthorized person.

TO modifications may be necessary during the TO period to address requirements or administrative changes. The OCO for each TO will administer the modifications for that TO. The contractor shall submit TO summary data and pricing tables, and shall forward copies of the complete TO as described in Section J.2.3 Task Order Data Management.

The contractor shall meet and comply with the processes, data and systems requirements to support and maintain TOs as described in Section J.2.3.

G.3.2.1 Task Order Award

All TOs awarded shall be placed directly by the OCO. Once awarded, the TO cannot be modified except by a TO modification.

G.3.2.2 Task Order Modification

Agencies that are subject to the federal acquisition regulation shall execute TO modifications in accordance with FAR Part 43.

The contractor shall report TO modifications to GSA as described in Section J.2.3 Task Order Data Management.

G.3.2.3 Protests and Complaints

Pursuant to FAR 16.505 (a)(9)(i) no protest is authorized in connection with the issuance or proposed issuance of an order under a TO contract, except for:

1. A protest on the grounds that the order increases the scope, period of performance, or maximum value of the contract.
2. A protest of an order valued in excess of $10 million.

GSA has appointed an ombudsman to review complaints from contractors and ensure they are afforded a fair opportunity to be considered. The ombudsman is a senior GSA official who is independent of the GSA CO and OCO.

G.3.2.3.1 Fair Opportunity Notice of Protest

Upon protesting a fair opportunity decision to the GAO, the agency, or an order ombudsman, the contractor shall provide a full un-redacted copy of that protest to the GSA CO within three (3) business days of the protest date. For FOIA requests the contractor shall provide a redacted copy to the GSA CO.

G.3.2.4 Customer of Record

The government may place orders under this contract with:

1. GSA acting as customer of record on behalf of another agency
2. The agency itself acting as customer of record
3. GSA acting as an OCO for an agency with the agency remaining as the customer of record

The contractor shall support all options.

G.3.2.5 Authorization of Orders

If a contractor does not have all mandatory services priced for a CBSA on its contract, and an agency issues a solicitation for a requirement in that CBSA, the contractor may not accept a TO or service order or provision services until all mandatory services for that CBSA have been added to its contract. If a contractor is missing a CBSA, the contractor may respond to a solicitation and then submit a modification for the missing CBSA in accordance with clause H.30 Expansion of Core Based Statistical Areas.

In addition to the CBSA requirement, if a contractor does not have a particular optional service on its contract, and an agency issues a solicitation including that service as a requirement, the contractor may submit a proposal or quote for the requirement provided it also submits a modification proposal to GSA to add the necessary services

to its contract and so indicates in the solicitation. The contractor shall not accept a TO or service order or provision services not on its contract.

In both cases (a missing CBSA or missing service), the contractor shall include a clear notice of the pending modification in its response to the solicitation.

For catalog items, if the contractor requires a new discount class as defined in B.1.3.1, it must submit a modification proposal to GSA to add the necessary discount class. If an agency issues a solicitation including an item that the contractor has identified as requiring a new discount class, the contractor may submit a proposal or quote for the requirement provided it also submits the modification proposal to GSA to add the necessary discount class to its contract and so indicates the required modification in the solicitation. The contractor shall not accept a TO or service order or provision catalog items until the discount class has been added to the contract.

If a contractor does not have a particular item on its catalog and an agency issues a solicitation including that item as a requirement, the contractor may submit a proposal or quote for the requirement. The contractor shall not accept a TO or service order or provision catalog items until the items have been added to the catalog.

G.3.3 Ordering Services

Within the limitations of the TO and the contract, the contractor shall accept orders for service incorporated directly within the TO or placed separately after the issuance of the TO. If an order for service incorporated directly within the TO is missing required data, with the exception of the data required in the TO as specified in Section G.3.2, the contractor shall accept supplemental information to complete the order.

This section describes the requirements for the placement, acceptance, and handling of all orders for service regardless of whether such orders are incorporated into the TO or placed separately after the issuance of the TO. In addition, process, data, and systems requirements for ordering service are described in Section J.2.4 Ordering.

Unless otherwise specified, all references to “orders” within this section refer to orders for service.

G.3.3.1 General Requirements for Ordering Services

G.3.3.1.1 Agency Hierarchy Code (AHC)

Orders submitted by the government will contain one or more Agency Hierarchy Codes (AHCs). The contractor shall reject any order submitted without an AHC for each line item. The contractor shall meet and comply with the AHC requirements as described in Section J.2.4.1.2 Agency Hierarchy Code.

G.3.3.1.2 Auto-Sold CLINs

If the contractor's solution to an agency requirement includes services with one or more auto-sold CLINs, as described in Section B.1.2.11 Auto-Sold CLINs, the contractor shall include those CLINs in the proposal or quote as though they had been expressly requested and ensure they are on the TO. All auto-sold CLINs shall be listed in all notifications and deliverables associated with an order. The contractor may add new auto-sold CLINs to the contract with GSA approval via a contract modification. Such newly added auto-sold CLINs shall not be applicable to any previously issued TO unless specifically added via TO modification. If a TO modification is issued to add a new auto-sold CLIN, the contractor shall issue new Service Order Completion Notices (SOCNs) for all applicable previously provisioned orders under that TO.

G.3.3.1.3 Customer Want Date

The order for services may include a Customer Want Date (CWD), which indicates the customer's desired install date. The contractor shall make reasonable effort to accommodate the CWD. If the order includes a CWD, the following requirements apply:

1. The contractor shall not issue the SOCN nor begin billing prior to the CWD unless the order specifies that early installation is acceptable.
2. If the time between the order and the CWD is greater than the defined provisioning interval for the service as described in Section G.8.2.2, the service provisioning SLA is waived for that service on that order.

NOTE: CWD specifications do not apply to rapid provisioning orders as described in Section G.3.3.3.2.

G.3.3.1.4 Service Order Completion Notification (SOCN)

After completion of each service provisioning the contractor shall submit a SOCN as described in Section J.2.4. After an order has been provisioned and a SOCN submitted and accepted, no revisions to the SOCN are permitted unless one of the following applies: the customer submits an administrative change order, to correct an erroneous submission with the prior approval of the COR, or to add or remove an auto-sold CLIN.

G.3.3.2 Order Types

G.3.3.2.1 Orders for New Services

Orders for new services are defined as orders for services (CLINs) that are not currently being provided.

G.3.3.2.2 Orders to Change Existing Services

G.3.3.2.2.1 Move Orders

Move orders are defined as orders that require the removal of an existing service and/or Service Related Equipment (SRE) from one location and the re-installation of the identical service and/or SRE at another location.

G.3.3.2.2.2 Feature Change Orders

Feature change orders are defined as orders that require changes to the features of an existing service as described in Section B. They fall into two categories:

- Feature changes that require a change to the CLIN being billed
- Feature changes that do not require a change to the CLIN being billed

G.3.3.2.2.3 Disconnect Orders

Disconnect orders are defined as orders that require the removal of services (CLINs) currently being provided. The contractor shall accept disconnect orders from agencies at any time. Billing for the disconnected services shall stop on the completion date in the SOCN and within the provisioning intervals for disconnects as specified in Section G.8 Service Level Management.

Disconnect orders will include the customer's desired disconnect date. If the time between the order and the customer's desired disconnect date is greater than the defined provisioning interval for the service as described in Section G.8.2.2, the service provisioning SLA will be waived for that service on that order.

The government will automatically stop payment on these orders based on the stated disconnect date.

Equipment related to disconnect orders shall be removed within 45 days after the termination of services. For equipment sanitization, see Section C.1.8.7.1.

If a disconnect order includes the disconnection of services that appear to leave other services effectively unusable (e.g., disconnecting a circuit but not the associated equipment), the contractor shall notify the customer of the full list of associated Unique Billing Identifiers (UBIs). The contractor shall request clarification of the customer's intent to only disconnect the specified service. If the customer provides instructions indicating that the list, in whole or in part, is intended for disconnect, the contractor shall accept this as an order update.

G.3.3.2.2.4 Administrative Change Orders

The contractor shall accept administrative changes to previously provisioned orders. After updating its system, the contractor shall provide the updated information to GSA as described in Section J.2.4.

Changes to administrative data associated with existing services can only occur based on an administrative change order. Administrative data is limited to data provided by the government that does not impact service delivery or pricing.

G.3.3.2.3 Updates to In-Progress Orders

Within the limitations defined in the subsections below, order line items that have not completed the provisioning process may be updated by the government to accommodate the following situations:

- Cancel the Order
- Change Service Delivery Location
- Change Service Features
- Change the Customer Want Date (CWD)
- Change in Administrative Data

G.3.3.2.3.1 Cancel Orders

The contractor shall accept an order from an agency to cancel a pending order at any step of the order process prior to SOCN.

If a cancel order includes the cancellation of services that appear to leave other services effectively unusable (e.g., canceling a circuit but not the associated equipment), the contractor shall notify the customer of the full list of order line items that are associated. The contractor shall request clarification of the customer's intent to only cancel the specified order line items. If the customer provides instructions indicating that the list, in whole or in part, is intended for cancellation, the contractor shall accept this as an order update.

The contractor shall not charge the ordering agency for network access orders if the cancellation order was placed 30 or more days before the later of:

1. The CWD in the initial order, or
2. The firm order commitment date.

If the government’s cancellation request does not meet the timeframe and requirements above, then the government shall pay the non-recurring charge (NRC) for the

associated access arrangements using the cancellation CLIN described in Section B.4.1.13, even if it was previously waived by the contractor.

G.3.3.2.3.2 Location Change Updates

Location change updates are defined as order updates that change the service delivery location from that specified in the original order. They fall into two categories:

- Changes in service delivery location that impact LEC provisioning.
- Changes in service delivery location that do not impact LEC provisioning.

G.3.3.2.3.3 Feature Change Updates

Feature change updates are defined as order updates that require changes to the features of an existing service. They fall into two categories:

- Feature changes that require a change to the CLIN originally ordered.
- Feature changes that do not require a change to the CLIN originally ordered.

G.3.3.2.3.4 Customer Want Date Change Updates

Customer Want Date (CWD) updates are defined as order updates that change the customer want date from that specified in the original order. If the agency delays the CWD prior to receiving the Firm Order Commitment Notice (FOCN), the contractor shall not issue the SOCN and begin billing prior to the new CWD, unless the change requested is less than14 days before the CWD of the initial order.

G.3.3.2.3.5 Administrative Data Change Updates

The contractor shall accept administrative changes to in-progress orders.

Administrative data is limited to data provided by the government that does not impact service delivery or pricing.

G.3.3.3 Special Order Handling

G.3.3.3.1 Telecommunications Service Priority (TSP) Orders

1. The contractor shall meet and comply with the requirements for Telecommunications Service Priority (TSP) orders (see Section G.11 National Security and Emergency Preparedness).

1. When TSP is specified in the order, the contractor shall provide the service in accordance with the following telecommunication service priority levels:

   a) PROVISIONING PRIORITY (5, 4, 3, 2, 1, or E),

   b) RESTORATION PRIORITY (5, 4, 3, 2, or 1), or

c) BOTH for both provisioning and restoration as specified in the order from Service Delivery Point to Service Delivery Point (SDP).

2. Restoration of service shall be in accordance with the TSP priority levels designated for the transmission service and in accordance with NCS Directive (NCSD) 3-1, TSP System for NS/EP and NCS Manual 3-1-1, "Service User Manual for the TSP System." NS/EP, including urgent or emergency delivery order service, shall be separately negotiated on an individual case basis.

3. Expedited service:

   a) The contractor shall provide expedited service implementation when the ordering agency requires priority provisioning for NS/EP circumstances or other circumstances in which the TSP system is invoked.

   b) The contractor shall make best effort to implement the ordered service(s) by the CWD, based on essential priorities as set certified by the DHS Program.

G.3.3.3.2 Rapid Provisioning Orders

Certain services, including self-provisioned services, lend themselves to rapid provisioning, which streamlines the provisioning process and only requires the Service Order Acknowledgement (SOA) and SOCN. If the contractor completes the provisioning process and issues a SOCN within twenty-four (24) hours of order submission, the SOA is not required.

An order is subject to rapid provisioning if all the following conditions apply:

1. The service ordered is specified as subject to rapid provisioning in the contract or the TO.
2. The order does not contain a TSP (see Section G.3.3.3.1).
3. The order does not contain an Administrative Change Order (see Section G.3.3.2.3.5).

As part of its proposal, the contractor shall specify which services it is offering as subject to rapid provisioning and the defined provisioning interval for each such service. The following restrictions apply to the contractor-defined provisioning intervals for rapid provisioning:

1. The provisioning interval shall not exceed 48 continuous hours.
2. The proposed provisioning interval shall be used to calculate SLA compliance as described in Section G.8.2.2.
3. Any CWD (see Section G.3.3.1.3) specified in the order does not apply, and early installation is acceptable.

G.3.3.3.3 Task Order Projects

The agency will indicate in the TO requirements whether the service orders under that TO are to be managed as a Task Order Project.

At the agency's discretion, upon award of the TO, the contractor shall prepare a Task Order Project Plan (TOPP). This plan identifies the contractor's project management processes, scheduling, procedures, tools, and implementation of the TO on the contractor's network. The contractor shall deliver the TOPP to the OCO of the TO (or service order) for approval and signature; the OCO's signature indicates agreement to the implementation schedule and as-of billing date for each item in the TO.

For each Task Order Project, the contractor shall provide the OCO with a single point of contact for service implementation. The contractor shall ensure that the point of contact or the designated alternate is accessible by telephone (office or mobile) or pager during the time periods when service implementation activities are taking place. The contractor shall coordinate with the OCO, customers, subcontractors, vendors, and other service providers during the service implementation. The contractor shall inform the OCO and the LGC on the order when activities, including installation and cutover testing, are scheduled at a building. If the contractor changes the installation or activation date, the contractor shall notify the OCO and provide a revised date.

Unless the OCO requests an alternative outline, the contractor shall include in the TOPP at a minimum the following information, and any additional information the contractor deems appropriate:

1. Name and information for the contractor's primary point of contact for implementing the plan and coordinating with the agency as well as escalation contacts.
2. Name of the OCO who awarded the TO.
3. The TO number.
4. Description of the specific activities required by all parties, including the contractor, the agency, vendors, and the incumbent service provider, to implement the project.
5. Specification of government equipment (hardware/software) required by location for this project.
6. Key areas of risk for the specific project, the contractor's processes and procedures to minimize risk, and the contingency plan to fallback to previous services, if any, in the event of failure of newly installed services.

7. Comprehensive inventory of services to be implemented along with SDP, proposed activation date, as-of billing date, testing and acceptance timeframes by the contractor and by the customer, and approach to implementation, such as hot-cutover or parallel operation.
8. Installation and service implementation schedule and as-of billing dates.
9. If applicable, interconnectivity or network gateways required for the implementation.
10. Any special technical requirements.
11. A site-specific design plan to include:
    a) Site preparation and implementation requirements for each building. Identify where site surveys will be required, whether surveys will be conducted via physical site visits, telephonically, or other means, and what information will be collected. Indicate what the ordering agency's responsibilities will be for site surveys.
    b) Interim and final configuration to include hardware (type, manufacturer, model), software, special circuit arrangements, environmental and electrical requirements, equipment room layouts, Main/Intermediate Distribution Frame / riser cable diagrams (if needed), and any special design requirements.
    c) Numbering plan and dialing plan. Identify blocks of telephone numbers, if any, that will have to change.
    d) Interface equipment for CPE, including identification and location of special systems integration requirements.
    e) A site-specific cutover test plan that describes the contractor's general approach to cutover testing and pass/fail criteria for each service during service implementation as described here and in Section E Inspection and Acceptance.

G.3.4 Testing and Acceptance of Services Ordered

The contractor shall meet and comply with the requirements for the verification testing of all associated EIS services based on the methodology defined in Section E.2.2 EIS Services Verification Testing. The contractor shall also meet and comply with the criteria for acceptance testing defined by the agency on the TO.

G.3.5 Performance Management

For completion timeframes associated with orders for services as defined in Section G.3.3 Ordering Services, the contractor shall meet and comply with requirements for service provisioning intervals as defined in Section G.8 Service Level Management.

G.4 Billing

This section describes the billing process, which includes:

1. Submission of billing invoice data by the contractor (see FAR 2.101 for the definition of “invoice”).
2. Verification and validation of billing by the government.
3. Resolution of any billing disputes and adjustments.

In addition to the billing functional requirements described herein, the contractor shall meet and comply with the processes, data, and systems interface requirements described in Section J.2.5 Billing.

G.4.1 Billing Prerequisites

The following information must be taken into consideration by the contractor to process and deliver billing details and adjustments.

G.4.1.1 Billing Cycle

The contractor shall comply with the government’s billing period, which runs from the first through the last day of the calendar month. The contractor shall bill the government in arrears at the end of every month after providing services. All billing shall be rendered based on calendar month cycles.

G.4.1.2 Billing Start Date and End Date

The contractor shall submit the SOCN to the government prior to billing for the associated service. The SOCN contains the order completion date:

- For new services, this date is the billing start date
- For disconnected services, this date is the billing end date

Unless otherwise specified in the TO, the NRC price billed shall be that which was in effect at the time the service order was placed and the MRC shall be that which is in effect for the billing month.

The contractor shall begin billing both NRC and MRC on the billing start date with the following exceptions:

- The contractor shall not begin billing for services if the government rejects the services within three (3) days of receipt of the SOCN. A longer period for test and acceptance may be specified in the TO. If the SOCN is rejected, the contractor shall issue a new SOCN for services, with an updated order completion date, after correcting the reasons for rejection.

- A TO may also specify alternate billing start date requirements provided the adjustment does not violate the 90-day billing requirement described in Section G.4.1.3. In such cases, the contractor shall comply with the billing start date requirements specified in the TO.

G.4.1.3 90-Day Billing Requirement

The contractor shall submit a proper Billing Invoice (BI) deliverable (see Section J.2.5 Billing) for all services and SREs up to 90 days after issuance of the SOCN. The contractor shall not receive payment for a single billing charge or portion of a billing charge invoiced after 90 days. The OCO may waive this 90-day billing requirement on a case-by-case basis. This 90-day requirement applies to both initial invoicing and all billing adjustments.

G.4.1.4 Unique Billing Identifier

As described in Section J.2.5, the Unique Billing Identifier (UBI) shall be included on all billing. The contractor shall create and assign a UBI for each billed record and provide it with each of the component(s) associated with the record to identify all components of a billed service.

G.4.1.5 Agency Hierarchy Code

Orders submitted by the government will contain an AHC as described in Section G.3 Ordering. The contractor shall include the AHC for each line item in all billing. The contractor shall meet and comply with the AHC requirements as described in Section J.2.4. The government will not pay the contractor for any order billed without an AHC for each line item.

G.4.1.6 Agency Service Request Number

Orders submitted by the government may contain one or two Agency Service Request Numbers (ASRNs). If provided by the government, the contractor shall include ASRN data in billing records throughout the service lifecycle as described in Section J.2.4.

G.4.1.7 Electronic Billing

The government intends to use electronic invoicing for all TOs. In addition to the billing deliverables described in Section J.2.5, the contractor shall input invoice summary data into a designated government system. The contractor shall support input into any of the following systems as specified by the GSA CO:

- WebVendor
- Vendor and Customer Self Service (VCSS) system

- Invoice Processing Platform (IPP)
- Other systems as specified in the TO

The contractor shall not submit and the government will not accept paper invoices except as authorized by the OCO.

G.4.2 Direct Billing

The contractor shall bill the agency directly for all charges incurred by the agency and its sub-agencies in accordance with the TO. The contractor will be paid directly by the agency.

The contractor shall be responsible for collecting the AGF and remittance of the total AGF amount collected for the month to GSA by electronic funds transfer (EFT).

G.4.3 Billing Functional Requirements

In addition to the functional requirements below, the contractor shall comply with the processes, deliverables and data exchange requirements for billing as defined in Section J.2.5 Billing.

The contractor shall respond within seven (7) days to a billing inquiry.

G.4.3.1 Adjustments

In the event it is necessary to adjust a bill, the contractor shall follow the adjustment process described in Section J.2.5 Billing. The contractor shall apply the adjustment to the next available bill. In the event of a dispute, the Billing Disputes process shall apply (see Section G.4.4).

G.4.3.2 Monthly Billing Informational Memorandum

The contractor shall provide, as needed, a Monthly Billing Informational Memorandum to coincide with the monthly delivery of billing files. The Monthly Billing Informational Memorandum is a list of information that includes, but is not limited to, items that explain changes in billing, changes to data formats, and new services added to the billing, and issues pertaining to balancing charges.

G.4.4 Disputes

The dispute process shall apply under any of the following conditions:

1. The government disputes the content of a BI submitted by the contractor.
2. The government disputes the content of an Inventory Reconciliation (IR) submitted by the contractor.
3. The government disputes a SLACR response submitted by the contractor.

The GSA CO, OCO, or authorized ordering official may submit to the contractor a dispute notice as defined in Section J.2.6 Billing & Inventory Disputes. The GSA CO or the OCO may designate additional personnel or systems authorized to submit a dispute notice.

The contractor shall accept and process the government's disputes. The contractor shall comply with the processes, deliverables, and data exchange requirements described in Section J.2.6 Billing & Inventory Disputes. The government will accept and process the contractor's disputes. The contractor shall resolve all disputes within 180 days of the dispute notice. The government reserves the right not to make payment for disputes that have not been resolved within 180 days.

The following section describes the billing dispute process.

G.4.4.1 Billing Disputes Resolution

Billing disputes begin with the initial submission of the dispute and end with the mutually agreeable resolution of the dispute. Payment adjustments will be applied on the next available bill. The government may reject a bill in whole or in part within seven (7) days of receipt. If only part of an invoice is in dispute, the government will pay the remainder of the bill and withhold only the disputed amount. Upon dispute resolution, the contractor shall submit corrected billing on the next available bill. For more information, see Section H.32 Payments and Incorrectly Invoiced Items and Prompt Payment Clause 52.232-25. The following requirements apply to billing dispute resolution:

1. The contractor shall resolve billing disputes with the agency that submitted the dispute.
2. The contractor shall work to resolve disputes within 180 days of the dispute notice.
3. In cases where a complete resolution is not forthcoming, the contractor may submit partial resolutions (less than the total amount in dispute) to the agency for acceptance or rejection. Accordingly, the OCO will respond within fourteen (14) days to the contractor’s proposed resolution. Either party may escalate the dispute at any time to the OCO. In cases where the contractor and government agree on a portion of a dispute, the parties may make an adjustment to resolve the agreed-to portion(s) pending resolution of the remainder of the dispute.
4. Disputes that are not resolved within 180 days of the dispute notice or the approved extension time shall be escalated to the OCO.
5. Disputes escalated to an OCO will be resolved in accordance with FAR 52.233-1 (Disputes).

6. Once a dispute is resolved, the contractor shall process the associated adjustment ensuring that the debit or credit and the associated billing dispute identifier are clearly documented according to Section J.2.6 Billing & Inventory Disputes.
7. The contractor shall provide a monthly Dispute Report (DR) in accordance with Section J.2.6 Billing & Inventory Disputes.

G.4.5 Payment of a Bill by the Government

The contractor will be paid only for items and services that are issued, delivered, and accepted in accordance with this contract's ordering, billing, and payment procedures (see Section H.32 Payments and Incorrectly Invoiced Items).

Conditions of the government's acceptance of services are described in Section E.2.2 EIS Service Verification Testing. Billing shall be submitted monthly in accordance with Section G.4.1.7 Electronic Billing and Section J.2.5 Billing.

Upon the expiration of the contract or TO, the contractor shall submit a final billing invoice within 90 days unless the contractor requests and is granted an extension by the OCO in writing.

The government will start the Prompt Payment clock according to FAR Clause 52.232-25 when the detail billing has been delivered to the government (See Section G.4.2 Direct Billing).

G.4.6 Associated Government Fee

The contractor shall collect the AGF from customer agencies on a monthly basis throughout the life of the contract. The total amount of AGF collected for each month shall be remitted to GSA via EFT no later than 15th business day of the following month. See Section J.2.5 Billing for details including calculation methodology.

G.4.7 Electronic Funds Transfer

The contractor shall accept payment of bills via EFT. The contractor shall provide information required to receive payment via EFT.

G.4.8 Government Purchase Card Payments

The contractor shall accept payment via Government Purchase Card when authorized by the government for telecommunications purchases under this contract.

The contractor shall coordinate with its bank to obtain the appropriate Standard Industrial Classification code for the services provided under the contract and establish

its Government Purchase Card financial procedures with its financial institution to ensure acceptance of such payments for billing.

G.4.9 Rounding of Charges for Billing and AGF

The contractor shall round billing in accordance with Section J.2.5.1.6 Rounding.

G.4.10 Proration of Monthly Charges

The contractor shall prorate billing based on the number of days that the service is provided during the billing period in accordance with Section J.2.5.1.5 Proration.

G.4.11 Taxes, Fees and Surcharges

G.4.11.1 Separate Billing of Taxes, Fees and Surcharges

The contractor shall separate billing amounts for taxes, fees and surcharges. Taxes, fees and surcharges shall be provided as individual components or amounts on the BI, whether they are part of an original charge or an adjustment.

The agency may elect to request prices that include all taxes, fees and surcharges in its solicitation (see Sections H.14 and H.23 for specific guidance). In this case, the contractor shall bill the prices that were proposed, accepted and included in the TO.

G.4.11.2 Aggregated Taxes

The contractor shall include the aggregated tax for each line item in the billing invoice and shall also provide the detailed composition of the aggregated tax in the tax detail deliverable (see Section J.2.5.1.7 Taxes, Fees and Surcharges).

G.4.12 Billing Performance Objectives

The contractor shall submit accurate billing that meets the following performance objectives for billing data accuracy and billing charge accuracy:

1. All applicable data elements shall be included on the BI in accordance with Section J.2.10 Data Dictionary.
2. The BI shall have an associated SOCN for each order.
3. The information on the BI shall be consistent with that on the SOCN.
4. There shall be no duplicate records within the BI.
5. There shall be no records within the BI that represent charges being billed more than 90 days after the issuance of the SOCN unless waived as described in G.4.1.3 (Note: this requirement applies to both initial invoicing and all billing adjustments).

6. The price shall match the price(s) on the contract or TO.

G.4.12.1 Billing Data Accuracy Key Performance Indicator

The Billing Data Accuracy Key Performance Indicator (KPI) measures the accuracy of the data submitted in the BI deliverable and is based on the accuracy standards listed above. KPI calculation is done on billing invoice after a six-month holding period to allow for resolution of any disputes. In the calculation below, “billing data submission” refers to an entire BI submission.

Billing Data Accuracy KPI is calculated in two steps:

1. Count the number of line items in the billing data submission that meet the above criteria.
2. Divide the result from Step 1 by the total number of line items in the billing data submission, and express the answer as a percentage.

The Acceptable Quality Level (AQL) is 95%.

G.4.12.2 Billing Charges Accuracy Key Performance Indicator

The Billing Charges Accuracy KPI measures the accuracy of the charges (prices) submitted in the BI deliverable. KPI calculation is done on billing invoice after a six-month holding period to allow for resolution of any disputes. In the calculation below, “billing data submission” refers to an entire BI submission.

Billing Data Accuracy KPI is calculated in three steps:

1. For each line in the billing data submission, calculate the absolute value of the difference between the correct charge (C) and the submitted charge (S): |C – S|.
2. Calculate the sum of the individual line results from Step 1.
3. Divide the result from Step 2 by the absolute value of the total of the correct charges in the billing data submission, subtract from 1, and express the answer as a percentage.

The AQL is 95%.

G.5 Business Support Systems

G.5.1 Overview

To support this contract, the contractor shall have and maintain Business Support Systems (BSS). The contractor is encouraged to leverage its commercial systems to meet the BSS requirements. This requirement can be met by a single, integrated BSS or a combination of BSSs that meets the requirements specified in this section. The functions described below are the minimum that will require automation to meet the government's requirements for this contract.

G.5.2 Reserved

G.5.3 Technical Requirements

G.5.3.1 Web Interface

The contractor's BSS shall include a secure, user-friendly web interface suitable for human interaction with appropriate training as defined in Section G.10 Training. As noted in Section G.5.1 above, this requirement can be met with multiple web interfaces.

G.5.3.1.1 Web Interface Functions

At a minimum this interface shall support the following functions (see Section G.5.4 BSS Component Service Requirements for function explanations and references):

- Order Submission including Pricing Catalog.
- Trouble Ticketing.
- Inventory Management.
- Billing and Payment Management.

All other functions included in Section G.5.4 BSS Component Service Requirements are highly desired but not required.

G.5.3.1.2 Technology Standards

To the extent practical, the government desires a web interface solution that adheres to common industry standards. To that end, the web interface shall not require special software or plug-ins beyond standard web browsers with default built-in functionality. At a minimum, the following web browsers in their current and immediate previous versions (N-1) as well as any successor products shall be supported for all functions:

- Microsoft Internet Explorer/Microsoft Edge (desktop and mobile).
- Google Chrome (desktop and mobile).
- Mozilla Firefox (desktop and mobile).

- Apple Safari (desktop and mobile).

G.5.3.1.3 Accessibility

The contractor's BSS supplied under this contract constitutes Electronic and Information Technology (EIT), as defined in FAR 2.101, and must conform to the Standards for Section 508 of the Rehabilitation Act at 36 C.F.R. § 1194.1 and Appendices A, C and D to Part 1194.

The contractor shall have readily available a comprehensive list of all offered EIT products (supplies and services) that fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Standards for Section 508 of the Rehabilitation Act at 36 C.F.R. § 1194.1 and Appendices A, C and D to Part 1194.The contractor shall also identify the technical standards applicable to all products proposed. In addition, the contractor shall clearly indicate where this list with full details of compliance can be found (e.g., an exact web page location). The contractor shall ensure that the list is available on the contractor's website(s) within 30 days of Notice to Proceed (NTP).

The contractor shall ensure that all EIT products that are less than fully compliant are offered pursuant to extensive market research, which ensures that they are the most compliant products available to satisfy the solicitation's requirements.

If any EIT product proposed is not fully compliant with all the standards, the contractor shall specify each specific standard that is not met, provide a detailed description as to how the EIT product does not comply with the identified standard(s), and indicate the degree of compliance.

The contractor shall make the BSS Voluntary Product Accessibility Template (VPAT) available on its website (See http://www.itic.org/policy/accessibility) and shall directly address compliance with Section 508 in the following deliverables:

- BSS Development and Implementation Plan
- BSS Verification Test Plan
- ~~BSS Verification Test Results~~

G.5.3.2 Direct Data Exchange

The contractor's BSS shall include secure, automated mechanisms for direct transfer of detailed transaction data to the GSA Conexus. This data shall cover all elements detailed in Section G.5.4 BSS Component Service Requirements.

G.5.3.2.1 Direct Data Exchange Methods

The contractor's BSS shall initiate and process bidirectional automated exchange of management and operations data using the following methods:

- Web Services: Transactions over HTTPS via contractor Business to Business (B2B) Application Program Interfaces (APIs) for system-to-system data exchange between government and contractor systems. The contractor shall support XML over HTTPS using SOAP as the web services exchange mechanism. The transactions will be bi-directional. GSA Conexus will utilize X.509-based digital certificates to support mutual authentication and encryption, and HTTPS as the protocol for secure web services between contractor systems and GSA Conexus, observing the National Institute of Standards and Technology (NIST) SP 800-95 Guide to Secure Web Services as well as other references identified in NIST SP 800-53 R4 and GSA Web Application Security Guide 07-35.
- Secure File Transport Protocol (SFTP) Services: Transactions for file-based data exchange between government and contractor systems using government provided FTP service. The transactions will include transfer of data from the government to the contractor and from the contractor to the government.

Additional detail about the data exchange methods is specified in Section J.2.9.

G.5.3.2.2 Direct Data Exchange Formats

The contractor's BSS shall accept data transfers from the government and submit data to the government in the formats specified in Section J.2.9.

G.5.3.2.3 Direct Data Exchange Governance

GSA shall maintain and manage all approved data exchange format specifications, data schemas, and method descriptions. The government customer may specify additional data exchange requirements in the TO. Any changes or updates, to include timeframes for implementation, will be coordinated and negotiated between the government and the contractor.

Once the BSS is operational, the contractor shall not make any changes to the data exchange formats or methods without government approval via the established change control process (see Section G.5.5.1 BSS Change Control).

G.5.3.3 Role Based Access Control (RBAC)

The contractor shall collect user registration and RBAC information from the government customer. The contractor shall use this information to setup access control on its BSS as described in Section J.2.3.

G.5.3.4 Data Detail Level

The data provided by the BSS shall be sufficiently detailed to provide all data elements relating to the services listed in Section G.5.4 BSS Component Service Requirements as addressed in Section J.2.

As indicated in Section J.2, all BSS deliverables and reports shall be submitted in at least the following formats:

1. Human-Readable (see to J.2.9 for required file types) – made available via the web interface (Section G.5.3.1 Web Interface) unless otherwise specified in the TO.
2. Machine-Readable (see to J.2.9 for required file types) – as part of the direct data exchange described in Section G.5.3.2 Direct Data Exchange.

G.5.4 BSS Component Service Requirements

G.5.4.1 BSS Component Service Requirements Table

Service	Minimum Functionality	Specified in Section(s)
Customer Management	• User Training • Trouble Management	• Section G.10 Training • Section G.6.4.1 Trouble Ticket Management General Requirements
Financial Management	• Billing Management • Disputes • SLA Credit Management • Payment Management	• Section G.4 Billing • Section G.8 Service Level Management
Order Management	• Order Submission • Order Tracking	• Section G.3 Ordering
Inventory Management	• Inventory Management	• Section G.7 Inventory Management
Service Management	• Service Assurance • SLA Management	• Section G.6 Service Assurance • Section G.8 Service Level Management
Program Management	• Administration • Project Management • Reporting • Service Catalog	• Section G.9 Program Management • Section B.1.3 Catalog Pricing Requirements - General

G.5.5 BSS Development

The contractor shall submit a BSS Development and Implementation Plan with its proposal. This plan shall detail how the BSS to support the contract will be architected

and supported to meet GSA's requirements including the development timeline (if applicable).

Although the BSS is required to support this contract, the government will not pay for or otherwise finance the development or maintenance of the BSS. The contractor shall be solely responsible for all development, testing, and maintenance including, but not limited to, security validation, functional testing, and configuration control.

The contractor shall provide upgrades to its BSS at no additional cost to the government, as these upgrades become available to its commercial customers. BSS functional testing requirements are defined in Section E.2.1. BSS security testing requirements are defined in Section G.5.6.

G.5.5.1 BSS Change Control

A change to the BSS is subject to change control, as defined in this section, if it has an impact on any of the following:

- Web interface user experience that impacts Section 508 compliance (see Section G.5.3.1.3)
- Web interface user experience that requires additional training of government personnel
- Direct data exchange (see Section G.5.3.2.1)
- Ability of BSS to meet any specified requirements including those specified in a TO award
- System security

The contractor shall provide a BSS Change Control Notification to the government at least 30 days prior to all BSS changes regardless of their impact. In the event of an emergency change, the contractor shall notify the government as soon the contractor discovers that a change is required.

For those changes that meet the standard for being subject to change control, the contractor shall:

1. Obtain government approval before implementing the change.
2. Use industry-standard change control procedures.
3. Train government personnel if required.
4. Retest with the government to ensure functionality continues to meet requirements. Relevant BSS testing must be successfully completed for any new functionality that impacts GSA Conexus before it becomes operational.

5. Update all relevant service documents and information posted on the contractor's website(s) as necessary, at no additional cost to the government and within seven (7) days of completing the change.

G.5.6 BSS Security Requirements

The contractor shall ensure security requirements are met for the BSS as defined in the BSS System Security Plan (BSS SSP) (see Section G.5.6.4), at a Moderate impact level and shall support government security and authorization efforts. The contractor shall also support the government's efforts to verify that these standards are being met.

G.5.6.1 General Security Compliance Requirements

In providing services under this contract, the contractor shall be subject to all current applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements. The contractor shall comply with Federal Information Security Management Act (FISMA) guidance and directives to include Federal Information Processing Standards (FIPS), NIST Special Publication (SP) 800 series guidelines (see http://csrc.nist.gov/), GSA IT security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of government IT. Compliance references shall include:

- Federal Information Security Management Act (FISMA) of 2002, available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
- Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.) available at: https://www.congress.gov/113/bills/s2521/BILLS-113s2521es.pdf.
- Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996," available at: https://www.fismacenter.com/clinger%20cohen.pdf.
- Privacy Act of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and contractors," August 27, 2004; available at: http://www.idmanagement.gov/.
- OMB Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended; available at: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/.
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies." (Available at: http://www.whitehouse.gov/omb/memoranda_2004).

- OMB Memorandum M-05-24, “Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors.” (Available at https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf.)
- OMB Memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors.” (Available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf.)
- OMB Memorandum M-14-03, “Enhancing the Security of Federal Information and Information Systems.” (Available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.)
- FIPS PUB 199, “Standards for Security Categorization of Federal Information and Information Systems.”
- FIPS PUB 200, “Minimum Security Requirements for Federal Information and Information Systems.”
- FIPS PUB 140-2, “Security Requirements for Cryptographic Modules.”
- NIST SP 800-18, Revision 1, “Guide for Developing Security Plans for Federal Information Systems.”
- NIST SP 800-30, Revision 1, “Guide for Conducting Risk Assessments.”
- NIST SP 800-34, Revision 1, “Contingency Planning Guide for Federal Information Systems.”
- NIST SP 800-37, Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.”
- NIST SP 800-39, “Managing Information Security Risk: Organization, Mission, and Information System View.”
- NIST SP 800-41, Revision 1, “Guidelines on Firewalls and Firewall Policy.”
- NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems.”
- NIST SP 800-53, Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations.”

- NIST SP 800-53A, Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.”
- NIST SP 800-61, Revision 2, “Computer Security Incident Handling Guide.”
- NIST SP 800-88, Revision 1, “Guidelines for Media Sanitization.”
- NIST SP 800-128, “Guide for Security-Focused Configuration Management of Information Systems.”
- NIST SP 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations.”
- NIST SP 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.”

In addition to complying with the requirements identified in the government policies, directives and guides specified above, the contractor shall comply with the current GSA policies, directives and guides listed below (the current documents are referenced within the GSA IT Security Policy and are available upon request submitted to the GSA CO*)*:

- GSA Information Technology (IT) Security Policy, CIO P 2100.1(J).
- GSA Order CIO P 2181.1 “GSA HSPD-12 Personal Identity Verification and Credentialing Handbook.”
- GSA Order CIO 2104.1, “GSA Information Technology (IT) General Rules of Behavior.”
- GSA Order CPO 1878.1, “GSA Privacy Act Program.”
- GSA IT Security Procedural Guide 01-01, “Identification and Authentication.”
- GSA IT Security Procedural Guide 01-02, “Incident Response.”
- GSA IT Security Procedural Guide 01-05, “Configuration Management.”
- GSA IT Security Procedural Guide 01-07, “Access Control.”
- GSA IT Security Procedural Guide 01-08, “Audit and Accountability Guide.”
- GSA IT Security Procedural Guide 05-29, “IT Security Training and Awareness Program.”
- GSA IT Security Procedural Guide 06-29, “Contingency Planning Guide.”
- GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.”
- GSA IT Security Procedural Guide 06-32, “Media Protection Guide.”

- GSA IT Security Procedural Guide 07-35, “Web Application Security Guide.”
- GSA IT Security Procedural Guide 08-39, “FY 2014 IT Security Program Management Implementation Plan.”
- GSA IT Security Procedural Guide 10-50, “Maintenance Guide.”
- GSA IT Security Procedural Guide 11-51, “Conducting Penetration Test Exercise Guide.”
- GSA IT Security Procedural Guide 12-63, “GSA’s System and Information Integrity.”
- GSA IT Security Procedural Guide 12-64, “Physical and Environmental Protection.”
- GSA IT Security Procedural Guide 12-66, “Continuous Monitoring Program.”
- GSA IT Security Procedural Guide 12-67, “Securing Mobile Devices and Applications Guide.”
- GSA IT Security Procedural Guide 14-69, “SSL / TLS Implementation Guide.”
- NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing December 2011.
- The Committee on National Security Systems Instruction (CNSSI) No. 5000, “Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony,” October 17, 2016.

G.5.6.2 GSA Security Compliance Requirements

FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems,” is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in eighteen security-related areas. Contractor systems supporting GSA must meet the minimum security requirements through the use of the security controls in accordance with NIST SP 800-53 R4.

To comply with the federal standard, GSA has determined the security category of the information and information system in accordance with FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems,” to be established at the Moderate Impact Level and baseline security controls must be established as identified in NIST SP 800-53 R4 and other associated directives and guides identified and/or provided by GSA. The contractor shall submit a Risk Management Framework Plan describing its approach for BSS security compliance.

This plan shall be submitted with the proposal in accordance with NIST SP 800-37. (Reference: NIST SP 800-37 R1, and NIST SP 800-53 R4: SA-3, RA-3).

G.5.6.3 Security Assessment and Authorization (Security A&A)

The implementation of an IT system to process federal government data requires a formal approval process known as Assessment and Authorization (A&A). NIST SP 800-37, Revision 1 (hereinafter listed as NIST SP 800-37) and GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk," provides guidance for performing the security A&A process. The contractor's system must have a valid security A&A prior to being placed into operation and processing government information. Failure to maintain a valid security A&A will be grounds for termination of the contract. The system must have a new security A&A conducted at least every three (3) years, or when there is a significant change that impacts the system's security posture.

G.5.6.4 BSS System Security Plan (BSS SSP)

The contractor shall comply with all security A&A requirements as mandated by federal laws, directives and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The level of effort for the security A&A is based on the system's NIST FIPS Publication 199 categorization. The BSS SSP shall be completed in accordance with NIST SP 800-18, Revision 1 (hereinafter listed as NIST SP 800-18) and other relevant guidelines. The BSS SSP for the information system shall initially be completed and submitted within 30 days of the NTP to include annual updates (Reference: NIST SP 800-53 R4: PL-2). At a minimum, the contractor shall create, maintain and update the following security A&A documentation:

1. The contractor shall develop and maintain a Security Assessment Boundary and Scope Document (BSD) as identified in NIST SP 800-37. This document will be used to determine the actual security assessment boundary. The set of information resources allocated to an information system defines the boundary for that system. These resources support the same mission/business objectives or functions. Generally the set of information resources is located within the same operating environment; however, distributed systems can reside in various locations with similar operating environments. Establishing and/or changing information system security boundaries is a cooperative effort between the federal government and the contractor. A template is available in Section J.8. The BSD for the information system shall intially be completed and submitted within 15 days of the NTP to include annual updates. (Reference: NIST SP 800-37 R1).

2. The contractor shall develop and maintain Interconnection Security Agreements (ISA) developed in accordance with NIST SP 800-47. The contractor shall provide any ISAs for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CA-3).
3. The contractor shall develop and maintain a GSA NIST SP 800-53 R4 Control Tailoring Workbook as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." A template is included in Section J.8. Column E of the workbook titled "Contractor Implemented Settings" shall document all contractor-implemented settings that are different from GSA-defined settings, and where GSA-defined settings allow a contractor to deviate. The contractor shall provide a Control Tailoring Workbook for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: AC-1).
4. The contractor shall develop and maintain a GSA Control Summary Table for a Moderate Impact Baseline as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." A template is provided in Section J.8. The contractor shall provide a GSA NIST SP 800-53 R4 Control Summary Table for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: AC-1).
5. The contractor shall develop and maintain a Rules of Behavior (RoB) for information system users as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk" and GSA Order CIO 2104.1, "GSA IT General Rules of Behavior." The contractor shall provide an RoB for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: PL-4).
6. The contractor shall develop and maintain a System Inventory that includes hardware, software and related information as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." The contractor shall provide a System Inventory for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CM-8).
7. The contractor shall develop and maintain a Contingency Plan (CP) including Disaster Recovery Plan (DRP) and Business Impact Assessment (BIA) completed in agreement with NIST SP 800-34. The contractor shall provide a CP, DRP, and BIA for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CP-2).

8. The contractor shall develop and maintain a Contingency Plan Test Plan (CPTP) completed in agreement with GSA IT Security Procedural Guide 06-29, “Contingency Planning Guide.” The contractor shall provide an CPTP for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CP-4).
9. The contractor shall test the CP and document the results in a Contigency Plan Test Report (CPTR), in agreement with GSA IT Security Procedural Guide 06-29, “Contingency Planning Guide.” The contractor shall provide a CPTR for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CP-4).
10. The contractor shall perform a Privacy Threshold Assessment (PTA)/Privacy Impact Analysis (PIA) completed as identified in GSA IT Security Procedural Guide 06-30, Managing Enterprise Risk. The contractor shall provide a PTA/PIA for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: AR-2, AR-3 and AR-4).
11. The contractor shall develop and maintain a Configuration Management Plan (CMP) (Reference: NIST SP 800-53 R4 control CM-9; NIST SP 800-128; GSA CIO-IT Security 01-05). The contractor shall provide a CMP for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CM-9).
12. The contractor shall develop and maintain a System(s) Baseline Configuration Standard Document (Reference: NIST SP 800-53 R4 control CM-2; NIST SP 800-128; GSA CIO-IT Security 01-05). The contractor shall provide a well defined, documented, and up-to-date specification to which the information system is built. The contractor shall provide the System Baseline Configuration for the information system as a part of the CMP and shall be submitted with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CM-9).
13. The contractor shall develop and maintain System Configuration Settings (Reference: NIST SP 800-53 R4 control CM-6; NIST SP 800-128; GSA CIO-IT Security 01-05). The contractor shall establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems shall be configured in accordance with GSA technical guides, NIST standards, Center for Internet Security (CIS) guidelines

(Level 1), or industry best practices in hardening systems, as deemed appropriate by the AO. System configuration settings shall be included as part of the Configuration Management plan and shall be updated and/or reviewed on an annual basis. (Reference: NIST SP 800-53 R4: CM-9).

14. The contractor shall develop and maintain an Incident Response Plan (IRP) (Reference: NIST SP 800-53 R4 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02 “Incident Response”). The contractor shall provide an IRP for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: IR-8).
15. The contractor shall test the IRP and document the results in an Incident Response Test Report (IRTR) (Reference: NIST SP 800-53 R4 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02 “Incident Response”). The contractor shall provide an IRTR for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: IR-3).
16. Maintenance of the system security will be through continuous monitoring of security controls of the contractor’s system and its environment of operation to determine if the security controls in the information system continue to be effective over time and as changes occur in the system and environment. The contractor shall develop and maintain a Continuous Monitoring Plan to document how continuous monitoring of information system will be accomplished. Through continuous monitoring, security controls and supporting deliverables shall be updated and submitted to GSA per the schedules below. The submitted deliverables provide a current understanding of the security state and risk posture of the information systems. They allow GSA authorizing officials to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. The contractor shall provide a Continuous Monitoring Plan for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CA-7).
17. The contractor shall develop and maintain a Plan of Action and Milestones completed in agreement with GSA IT Security Procedural Guide 06-30, “Plan of Action and Milestones (POA&M).” All scans associated with the POA&M shall be performed as an authenticated user with elevated privileges. Vulnerability scanning results shall be managed and mitigated in the POA&M and submitted together with the quarterly POA&M submission. (Reference: NIST SP 800-53 R4; RA-5 and GSA CIO-IT Security Guide 06-30). Scans shall include all networking components that fall within the security accreditation boundary. The appropriate

vulnerability scans are also submitted with the initial security A&A package. An annual information system User Certification/Authorization Review must be annotated on the POA&M. A POA&M template is provided in Section J8. The contractor shall provide a POA&M for the information system as part of the initial security A&A package followed by quarterly updates. (Reference: NIST SP 800-53 R4; CA-5).

18. All FIPS 199 Low, Moderate and High impact information systems must complete an independent internal and external penetration test and provide an Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities with the security assessment package and on an annual basis in accordance with GSA CIO-IT Security Guide 11-51. GSA will provide for the scheduling and performance of these penetration tests. All penetration test exercises must be coordinated through the GSA Office of the Chief Information Security Officer (OSISO) Security Engineering (ISE) division at itsecurity@gsa.gov per GSA CIO-IT Security Guide 11-51. (Reference: NIST SP 800-53 R4; CA-5 and RA-5).
19. All FIPS 199 Low, Moderate, and High impact information systems must conduct code analysis reviews in accordance with GSA CIO Security Procedural Guide 12-66 using the appropriate automated tools (e.g., Fortify, Veracode, etc.) to examine for common flaws, and document results in a Code Review Report to be submitted prior to placing system into production, when there are changes to code and on an annual basis. Applicable NIST SP 800-53 R4 Control is SA-11. References: GSA CIO Security Procedural Guides 06-30, “Managing Enterprise Risk” and GSA CIO Security Procedural Guide 12-66, “Continuous Monitoring Program.” If applicable, a Code Review Report shall be submitted as an initial deliverable prior to placing the information system into production, when there are changes to code and on an annual basis. (Reference: NIST SP 800-53 R4: SA-11).
20. The government is responsible for providing the Security/Risk Assessment and Penetration Tests. The contractor shall allow GSA employees (or GSA-designated third-party contractors) to conduct security A&A activities to include control reviews in accordance with NIST SP 800-53 R4 / NIST SP 800-53A R4 and GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of government information. This includes the general support system infrastructure. All scans must be performed as an authenticated user with elevated privileges.

21. All identified gaps between required 800-53 R4 controls and the contractor's implementation as documented in the Security/Risk Assessment Report (SAR) shall be tracked by the contractor for mitigation in a POA&M document completed in accordance with GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)."
22. The contractor shall mitigate all security risks found during the security A&A and continuous monitoring activities. All critical and high-risk vulnerabilities shall be mitigated within 30 days and all moderate risk vulnerabilities shall be mitigated within 90 days from the date vulnerabilities are formally identified. The government will determine the risk rating of vulnerabilities. Updates shall be provided on a monthly basis on the status of all critical and high vulnerabilities that have not been closed within 30 days.
23. The contractor shall deliver the results of the annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26, "FISMA Implementation." Each fiscal year the annual assessment will be completed in accordance with instructions provided by GSA. (Reference: NIST SP 800-53 R4: CA-2).
24. The contractor shall develop and keep current all policy and procedures documents, as outlined in the specified NIST documents as well as appropriate GSA IT Security Procedural Guides . The following documents shall be verified and reviewed during the initial security assessment and updates provided to the GSA COR/ISSO/ISSM biennially:
    a) Access Control Policy and Procedures (NIST SP 800-53 R4: AC-1).
    b) Security Awareness and Training Policy and Procedures (NIST SP 800-53 R4: AT-1).
    c) Audit and Accountability Policy and Procedures (NIST SP 800-53 R4: AU-1).
    d) Security Assessment and Authorization Policies and Procedures (NIST SP 800-53 R4: CA-1).
    e) Configuration and Management Policy and Procedures (NIST SP 800-53 R4: CM-1).
    f) Contingency Planning Policy and Procedures (NIST SP 800-53 R4: CP-1).
    g) Identification and Authentication Policy and Procedures (NIST SP 800-53 R4: IA-1).
    h) Incident Response Policy and Procedures (NIST SP 800-53 R4: IR-1).
    i) System Maintenance Policy and Procedures (NIST SP 800-53 R4: MA-1).
    j) Media Protection Policy and Procedures (NIST SP 800-53 R4: MP-1).

k) Physical and Environmental Policy and Procedures (NIST SP 800-53 R4: PE-1).
l) Security Planning Policy and Procedures (NIST SP 800-53 R4: PL-1).
m) Personnel Security Policy and Procedures (NIST SP 800-53 R4: PS-1).
n) Risk Assessment Policy and Procedures (NISTSP 800-53 R4: RA-1).
o) Systems and Services Acquisition Policy and Procedures (NIST SP 800-53 R4: SA-1).
p) System and Communication Protection Policy and Procedures (NIST SP 800-53 R4: SC-1).
q) System and Information Integrity Policy and Procedures (NIST SP 800-53 R4: SI-1).

G.5.6.5 Reserved

G.5.6.6 Additional Security Requirements

The contractor shall ensure that proper privacy and security safeguards are adhered to in accordance with the FAR Part 52.239-1, see Section I.

The deliverables identified in Section G.5.6.4 shall be labeled "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) or contractor-selected designation per document sensitivity. External transmission/dissemination of Controlled Unclassified Information (CUI) data to or from a GSA computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "*Security Requirements for Cryptographic Modules.*"

Where appropriate, the contractor shall ensure implementation of the requirements identified in the FAR (see Section I, 52.224-1, "*Privacy Act Notification*" and FAR 52.224-2, "*Privacy Act*.")

The contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the federal government's agent.

The government has the right to perform manual or automated audits, scans, reviews, or other inspections of the contractor's IT environment being used to provide or facilitate services for the government. In accordance with the FAR (see Section I, 52.239-1) the contractor shall be responsible for the following privacy and security safeguards:

1. The contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the contractor under this contract or otherwise provided by the government (except for disclosure to a consumer agency for purposes of security A&A verification).

2. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public government data collected and stored by the contractor, the contractor shall provide the government logical and physical access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods:
    - Authenticated and unauthenticated operating system/network vulnerability scans
    - Authenticated and unauthenticated web application vulnerability scans
    - Authenticated and unauthenticated database application vulnerability scans
    - Internal and external penetration testing
3. Automated scans can be performed by government personnel, or agents acting on behalf of the government, using government operated equipment, and government specified tools. If the contractor chooses to run its own automated scans or audits, results from these scans may, at the government's discretion, be accepted in lieu of government performed vulnerability scans (See GSA Security Guide 6-30 "Managing Enterprise Risk" for acceptance criteria). In these cases, scanning tools and their configurations shall be approved by the government. In addition, the results of contractor-conducted scans shall be provided, in full, to the government.

G.5.6.6.1 Personnel Security Suitability

The contractor shall perform personnel security/suitability in accordance with FAR Part 52.204-9, see Section I.

All contractor personnel with access to government information that is within the security A&A scope must successfully complete a background investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12), OMB guidance M-05-24, M-11-11 and as specified in GSA CIO Order 2100.1J and GSA Directive 9732.1D Suitability and Personnel Security.

The government shall be responsible for the cost of such background investigations.

G.5.7 Data Retention

The contractor shall comply with FAR Subpart 4.7 (48 CFR 4.7), to maintain an archive of all records for three (3) years after final payment under the contract.

G.6 Service Assurance

This section describes the requirements for the following Service Assurance functions:

- Customer support
- Supply Chain Risk Management (SCRM)
- Trouble ticket management

G.6.1 Customer Support Office

The contractor's Customer Support Office (CSO) will be the primary interface between the contractor and government entities interested in or using the contract. The contractor shall identify the structure of the CSO to the government in the contract. The CSO shall support the contractor's sales, service and implementation activities with the government. The CSO will be set up to communicate with government users of the contract around the world using common means of communications including toll-free number, email, and collaboration tools.

The CSO shall assist users experiencing difficulty and shall provide training as required. The contractor shall also make Customer Service Representatives (CSRs) available to users for requirements planning or billing reconciliation.

G.6.2 Customer Support Office and Technical Support

The contractor's CSO shall be located at premises provided by the contractor and shall provide basic operation at contract award, with a main toll-free telephone number and primary email address. The contractor shall have all functional areas of the CSO fully operational within 30 days of NTP. The contractor's CSO shall:

1. Facilitate the government's use of the contract.
2. Provide contact information for each functional area of the CSO.
3. Respond to general inquiries.
4. Provide information regarding available products and services, respond to service inquiries, and accept orders.
5. Provide training registration and scheduling information.
6. Respond to inquiries via the same method the user used to access the CSO, unless otherwise specified by the user.
7. Provide a main US toll-free telephone number through which all CSO functional areas can be accessed.

8. Provide the capability for non-domestic users to contact the CSO without incurring international charges and minimize, to the extent possible, the different CSO contact numbers required to support non-domestic users.
9. Provide hot-links from the contractor's public EIS website(s) to CSO functional area email addresses.
10. Provide Telecommunications Device for the Deaf (TDD) access to the CSO for government representatives who are hearing impaired or have speech disabilities.
11. Deal effectively with the geographical distribution of EIS subscribing agencies, GSA's Program Management Offices (PMOs) in the GSA regions, and GSA international activities.
12. Provide responses to user inquiries of a general nature such as the contractor's established administrative and operational procedures, contractor points of contact, and user forum information.
13. Provide information on available training classes as well as guidance and assistance with registration for training classes. Training requirements are described in G.10 Training.
14. Provide technical support to agencies and the PMO regarding the services the contractor delivers to the government. Technical support shall include, but not be limited to:
    a) Answering questions related to how users can obtain the functions designed into the services the contractor provides via the contract
    b) Advising users on the capabilities incorporated into service features
    c) Providing technical support to assist either the contractor technicians or the agencies or other organizations or personnel in the timely resolution of troubles
    d) Notifying users of new services and features that are planned or that have recently been added to the contract
    e) Providing ordering and tracking support services
    f) Providing support to help resolve billing issues
    g) Providing inventory management support

G.6.3 Supply Chain Risk Management

The contractor shall include a SCRM Plan with its proposal that addresses counterfeit and illegally modified products. The SCRM plan shall describe the contractor's

approach to SCRM and demonstrate how the contractor's approach will reduce and mitigate supply chain risks.

The contractor shall provide a SCRM plan to manage supply chain risk throughout each of the five (5) supply chain phases specified in its proposal: 1) design and engineering, 2) manufacturing and assembly, 3) distribution and warehousing, 4) operations and support, and 5) disposal and return. In addition to the components and processes for which the contractor is directly responsible, and as feasible, the contractor shall identify "specified supporting infrastructure beyond the system boundary" and where appropriate, include such infrastructure in its SCRM Plan.

The SCRM Plan shall address at a minimum, but not be limited to, the following:

1. How the contractor ensures that requirements for genuine Information Technology Tools (ITT) are imposed upon its direct suppliers, whether the direct supplier is a systems integrator, reseller or OEM. The requirements for assurance and supporting evidence must include:
    a) The contractor performs reasonable steps to ensure its SCRM Plan is performed for ITT in its delivered and installed configuration.
    b) Equipment resellers from whom the contractor purchases ITT have valid licenses for OEM equipment and software.
    c) The ITT OEM exercises strict quality control to ensure that counterfeit or illegally modified hardware or software components are not incorporated into the OEM product.
    d) The contractor ensures traceability of assurance and evidence of genuineness of ITT back to the licensed product and component OEMs.
2. The contractor's use of system security engineering processes in specifying and designing a system that is protected against external threats and against hardware and software vulnerabilities.
3. The contractor's strategy for implementing SCRM security requirements throughout the life of the contract. The SCRM plan shall address the security controls described in NIST SP 800-53 R4 or the latest publication. Implementation of the controls shall be tailored in scope to the effort and the specific information.
4. The criticality analysis (CA) process used by the contractor to determine Mission Critical Functions and the protection techniques (countermeasures and sub-countermeasures) used to achieve system protection and mission effectiveness. The CA shall describe the contractor's supply chain for all critical hardware and software components (and material included in products), key suppliers, and

include proof of company ownership and location (on-shore or off-shore) for key suppliers and component manufacturers.

5. How the contractor will ensure that products and components are not repaired and shipped as new products and components provided to the government.
6. How the contractor will ensure that supply channels are monitored for counterfeit products throughout the product life cycle to include maintenance and repair.
7. How the contractor's physical and logical delivery mechanisms will protect against unauthorized access, exposure of system components, information misuse, unauthorized modification, or redirection.
8. How the contractor's operational processes (during maintenance, upgrade, patching, element replacement, or other sustainment activities) and disposal processes will limit opportunities for knowledge exposure, data release, or system compromise.
9. Which of the following identifies the relationship between the contractor and the manufacturer: 1) OEM, 2) authorized reseller, 3) authorized partner/distributor, or 4) unknown/unidentified source.
10. The contractor's expressed warranty that the software shall be free from all computer viruses, worms, trojans, time-outs, time bombs, back doors, disabling devices and other harmful or malicious code intended to or which may damage, disrupt, inconvenience or permit access to the software user's or another's software, hardware, networks, data or information. The government will only accept standard commerical warranties for Commerical-Off-the-Shelf (COTS) components only if they are consistent wtih clause 52.246.17. In the case of standard commerical warranties that exceed one year, the government shall receive the additional term(s) of the commerical warranty.
11. How the contractor will ensure independent verification and validation of assurances, and provide supporting evidence as required.

The contractor shall incorporate the substance of this clause in subcontracts at all tiers where a subcontractor provides personnel, components, or processes identified as 1) a critical component, or 2) part of the contractor's supporting infrastructure. All subcontractors providing critical components or services shall be identified and required to provide all necessary information to complete the SCRM Plan in association with the contractor. Suppliers of COTS components are considered subcontractors for this contract.

The contractor shall comply with NIST SP 800-161 Supply Chain Risk Management (SCRM) Practices. The offeror shall update its SCRM Plan to include any future

changes to the NIST SCRM Guidelines and all such modifications to the Plan shall be made at no cost to the government.

G.6.3.1 Plan Submittal and Review

The plan shall be submitted with the contractor's proposal. Updates shall be submitted on an annual basis to the CO and COR. All information included will be treated as Controlled Unclassified Information pursuant to Executive Order 13556, shared only with government agencies, and used solely for the purposes of mission essential risk management. All reviews shall be completed within a 45-day time period.

G.6.4 Trouble Ticket Management

The contractor shall perform trouble ticket management in accordance with commercial best practices, and shall meet the government's requirements specified below.

G.6.4.1 Trouble Ticket Management General Requirements

The contractor shall create a trouble ticket for any reported and discovered service issues, provide status updates, provide online real-time access to trouble ticketing and system status information, update open trouble tickets and escalate as needed, and report the resolution to the initiator.

The contractor shall establish and implement procedures and systems for 24x7x365 trouble ticket and complaint collection, entry, tracking, analysis, priority classification, and escalation for all services to ensure that problems are resolved within the timeframes specified in Section G.8 Service Level Management.

As the first priority, the contractor shall restore any TSP restoration coded service, as quickly as possible, using best effort.

The contractor shall escalate issues according to the contractor's Program Management Plan (PMP) as described in Section G.9.4 Program Management Plan.

G.6.4.2 Reporting Information

The contractor shall provide the government with the capability to query, sort, export, and save in formats such as PDF/CSV or standard/structured file formats trouble and complaint records by any field or combination of formatted (that is, not free-form text) fields in each record.

The contractor shall process any credits applicable to the service outage based on this record of information. SLAs and credits are defined in Section G.8 Service Level Management.

The contractor shall, upon request from the PMO and agencies, deliver archived trouble and complaint report data within five (5) days of the request for such information.

G.7 Inventory Management

G.7.1 Inventory Management Process Definition

The contractor shall establish, and keep current a complete and accurate inventory of EIS services provided to agencies. The contractor shall provide a secure web interface to allow the government to access the data, make queries, obtain reports and perform periodic downloads as needed for audits, billing verification, and other government program management purposes. The technical details for this interface are defined in Section G.5.3.1 Web Interface.

The key tasks associated with inventory management are defined below:

1. GSA identifies the minimum inventory data elements required by service as part of the Inventory Reconciliation (IR) deliverable and specified in Section J.2.7 Inventory Management.
2. As new or enhanced services are added by contract modification, additional inventory data elements will be added to the IR deliverable.
3. The government audits the EIS inventory data provided and advises the contractor of discrepancies noted in the EIS inventory data.
4. The contractor shall investigate EIS inventory data discrepancies reported by the government and works with the government to resolve them.
5. The contractor shall make corrections to the EIS inventory as needed to maintain its accuracy and completeness and issues corrected SOCNs or billing as needed.
6. The contractor shall meet the inventory requirements for transition as defined in Section C.3 Transition.

G.7.1.1 Inventory Management Functional Requirements

The key functional requirements related to Inventory Management are described below:

1. The contractor shall fully populate the EIS Inventory with the data elements of the IR as defined in Section J.2.7 Inventory Management.
2. The contractor shall initially populate records of EIS services in the EIS inventory within one (1) business day of the issuance of SOCNs for EIS services delivered to customers.
    a) The contractor shall establish an inventory for all EIS services provided to its customers.

b) The contractor shall maintain and update the EIS inventory for all EIS services provided to its customers.

c) The contractor shall make the EIS inventory data available to the government.

3. The contractor shall deliver IR deliverable each month as defined in Section J.2.7 Inventory Management.

G.7.1.2 EIS Inventory Maintenance

1. The contractor shall maintain and update the EIS Inventory for all EIS services provided to its customers.
2. The contractor shall update the EIS inventory current view to reflect all additions, deletions, or changes to the EIS services being provided within one (1) business day of the issuance of the SOCN for every addition, deletion, or change.

G.7.1.3 EIS Inventory Data Availability

The contractor shall:

1. Provide to government users secure electronic access to the current view and to the monthly snapshots of EIS services in the contractor-maintained EIS inventory.
2. For secure web-based queries against the contractor-maintained EIS inventory, the contractor shall, as a minimum:

   a) Provide government users the option to select a user choice of online viewing, data file downloading.

   b) Provide and maintain on its EIS BSS web interface a link for secure, electronic access to the contractor-maintained EIS inventory information.

3. For data export or data file delivery in response to a secure query against the contractor-maintained EIS inventory, the contractor shall, at a minimum:

   a) Support common industry standard formats and file structures

   b) Impose no limit on the number of records that is less than the limit imposed by the file format specification

4. Make older monthly snapshots of the EIS inventory that have been archived available for query access, within five (5) days of a government request.
5. Retain the monthly snapshots of the EIS inventory and provide them to the government as requested for three (3) years following the expiration or termination of the contract.

6. Meet or exceed the access security and performance requirements specified in Section G.5.6 BSS Security Requirements for the system used for the EIS inventory.
7. If requested by the government, the contractor shall, at no additional expense to the government, provide a copy of the records, in the format requested by the government, with data field labels, in the current EIS inventory or any of the monthly snapshots either in their entirety or for a subset specified in the government's request.
8. If requested by the government, the contractor shall, at no additional expense to the government, provide a copy of the records in the current EIS inventory, in the format requested by the government, in their entirety of for a subset specified in the government's request.
9. The contractor shall not restrict the use by the government of any and all EIS inventory data related to this contract during the contract and for three (3) years following the expiration or termination of the contract.

G.7.1.4 EIS Inventory Data Discrepancies and Accuracy

G.7.1.4.1 EIS Inventory Data Discrepancies

1. The contractor shall investigate EIS inventory data discrepancies reported by the government. If the contractor agrees to a correction, it shall correct the data discrepancies within ten (10) days.
2. If the contractor does not agree to a correction, it shall advise the government and work with the government to resolve the issue.
3. If the discrepancy is escalated to the CO for resolution, the contractor shall work with the CO to resolve the issue to the government's satisfaction.

G.7.1.4.2 EIS Inventory Data Accuracy

1. The contractor shall institute internal verification and audit procedures to ensure that the EIS inventory is complete and correct.
2. When the contractor discovers an EIS inventory data discrepancy, agrees with a government report of a discrepancy, or is directed to do so by the CO, the contractor shall correct its EIS inventory at no additional cost to the government.
3. When the contractor discovers an EIS inventory data discrepancy, agrees with a government report of an EIS inventory data discrepancy, or is directed to do so by the CO as a result of formal discrepancy resolution, the contractor shall also

investigate whether or not the EIS inventory data elements in the SOCN or Billing Detail (BD) deliverable issued to the government were correct or in error.

4. If the EIS inventory data elements in the SOCN issued to the government were in error, the contractor shall issue, at no additional cost to the government, a corrected SOCN or a new correct SOCN that clearly references the original error.
5. If the EIS inventory data elements result in a billing error in the BD deliverable issued to the government, the contractor shall issue, at no additional cost to the government, a Billing Adjustment (BA) deliverable.
6. The contractor shall correct data discrepancies as they occur and as designated by the government within ten (10) days.

G.7.1.5 EIS Inventory Reconciliation

The contractor shall provide the monthly IR deliverable as defined in Section J.2.7 Inventory Management.

G.8 Service Level Management

This section defines the approach to Service Level Management to be used under the contract. This section specifically addresses the following:

- Service Level Agreements (SLAs)
- Methodological approach to managing those metrics
- SLA reporting requirements

The contractor is responsible for services provided by its subcontractors and any other providers that the contractor uses to deliver EIS services.

G.8.1 Overview

An SLA is an agreement between the government and the contractor to provide a service at a performance level that meets or exceeds the specified performance objective(s). The contract has specific KPIs for nearly all services. If a contractor does offer a service, it must comply with those KPIs. For each KPI, the contractor shall meet specified AQLs. Certain services deemed essential to government operations also require mandatory SLAs. If the specified service levels are not met, then the contractor shall issue specified credits.

This section contains the following major components:

- Service Level Agreement Tables (all SLAs under the contract)
- Service Level General Requirements
- SLA Credit Management Methodology
- Service Level Reporting Requirements

G.8.2 Service Level Agreement Tables

This section contains all standard SLAs. If the contractor offers a service, or if a service is included on a TO, the following SLAs shall apply.

The SLAs in this document represent a minimum level of service acceptable to the government unless otherwise specified at the TO level. Agencies may define additional or different SLAs, KPIs and AQLs during the TO process. These TO-specific SLAs are equally binding, and the contractor is subject to the terms and conditions stated after agreeing to the measurement and price.

G.8.2.1 Service Performance SLAs

G.8.2.1.1 Service-Specific SLAs

Service-specific SLAs are performance measures demonstrating the overall performance of a single TO service. The following table lists each service SLA and a reference to the appropriate location in Section C Technical Requirements. The referenced portion of Section C contains the associated KPIs, their definitions, measurement methodologies, and AQLs. The SLA is defined by all KPIs listed for the service in Section C except those for Time-to-Restore which are addressed in Section G.8.2.1.2.~~The following table lists each service SLA, the KPIs that define the SLA, and a reference to the appropriate location in Section C Technical Requirements. The referenced portion of Section C contains KPI definitions, their measurement methodologies, and their AQLs.~~ For each service SLA the contractor is required to meet the AQL associated with each KPI listed. The KPIs shall be measured and reported for each unique instance of a service which is defined at the most granular level to which the KPI is applicable but never at a level higher than that defined by the UBI service grouping (see Section J.2.10.1.1.2).

Failure to meet the AQL for any KPI within an SLA constitutes failing that SLA.

G.8.2.1.1.1 Service-Specific SLA Table

Service	Service ID	~~KPIs Defining the Service-Specific SLA~~	Section C Reference
Virtual Private Network Service	VPNS	~~• Latency (CONUS)~~ ~~• Latency (OCONUS)~~ • ~~Availability (VPN)~~	C.2.1.1.4
Ethernet Transport Service	ETS	~~• Availability (ETS) – Routine~~ ~~• Availability (ETS) – Critical~~ ~~• Latency (ETS) (CONUS)~~ ~~• Latency (ETS) (OCONUS)~~ ~~• Jitter (Packet)~~ ~~• Grade of Service (Packet Delivery Rate) – Routine~~ ~~• Grade of Service (Packet Delivery Rate) – Critical~~ ~~• Grade of Service (Failover Time) - Routine~~ • ~~Grade of Service (Failover Time) - Critical~~	C.2.1.2.4
Optical Wavelength Service	OWS	~~• Availability (OWS over WDM) – Routine~~ ~~• Availability (OWS over WDM) – Critical~~ ~~• Grade of Service (Restoration Time) - Routine~~ • ~~Grade of Service (Restoration Time) - Critical~~	C.2.1.3.4

Service	Service ID	~~KPIs Defining the Service-Specific SLA~~	Section C Reference
Private Line Service	PLS	~~• Availability (POP-to-POP) – Routine~~ ~~• Availability (POP-to-POP) – Critical~~ ~~• Availability (SDP-to-SDP) – Routine~~ • ~~Availability (SDP-to-SDP) – Critical~~	C.2.1.4.4
Synchronized Optical Network Service	SONETS	~~• Availability (SONETS) (SDP-to-SDP) – Routine~~ • ~~Availability (SONETS) (SDP-to-SDP) – Critical~~	C.2.1.5.4
Dark Fiber Service	DFS	~~• Attenuation Coefficient SMF (1550 nm)~~ ~~• Attenuation Coefficient SMF (1310 nm)~~ ~~• Attenuation Coefficient MMF 850 nm (50/125 µm)~~ ~~• Attenuation Coefficient MMF 1300 nm (50/125 µm)~~ ~~• Polarization Mode Dispersion at 1550 nm (Inter-City Networks)~~ ~~• Polarization Mode Dispersion (Intra-City Networks)~~ ~~• Chromatic Dispersion at 1550nm~~ ~~• Reflectance Events (all events)~~ ~~• Connectors Loss SMF~~ ~~• Fusion Splicing Loss SMF~~	C.2.1.6.4
Internet Protocol Service	IPS	~~• Availability (Port) – Routine~~ ~~• Availability (Port) – Critical~~ ~~• Latency (CONUS) – Routine~~ ~~• Latency (CONUS) – Critical~~ ~~• GOS (Data Delivery Rate) – Routine~~ • ~~GOS (Data Delivery Rate) – Critical~~	C.2.1.7.4
Internet Protocol Voice Service	IPVS	~~• Latency~~ ~~• Grade of Service (Packet Loss)~~ ~~• Availability – Routine~~ ~~• Availability – Critical~~ ~~• Jitter~~ • ~~Voice Quality~~	C.2.2.1.4
Circuit Switched Voice Service	CSVS	~~• Availability (POP-to-POP) – Routine~~ ~~• Availability (SDP-to-SDP) – Routine~~ ~~• Availability (SDP-to-SDP) – Critical~~ ~~• Grade of Service (Call Blockage) – Routine~~ • ~~Grade of Service (Call Blockage) – Critical~~	C.2.2.2.4
Toll Free Service	TFS	~~• Availability (POP-to-POP)~~ ~~• Availability (POP-to-terminating-SDP) – Routine~~ ~~• Availability (POP-to-terminating-SDP) – Critical~~ ~~• Grade of Service (Call Blockage) – Routine~~ • ~~Grade of Service (Call Blockage) – Critical~~	C.2.2.3.4

Service	Service ID	~~KPIs Defining the Service-Specific SLA~~	Section C Reference
Circuit Switched Data Service	CSDS	~~• Availability (POP-to-POP)~~ ~~• Availability (SDP-to-SDP) – Routine~~ ~~• Availability (SDP-to-SDP) – Critical~~ ~~• Grade of Service (Call Blockage) – Routine~~ • ~~Grade of Service (Call Blockage) – Critical~~	C.2.2.4.4
Contact Center Service	CCS	~~• Availability – Routine~~ • ~~Availability – Critical~~	C.2.3.1.7
Co-located Hosting Center Service	CHS	• ~~Internet Availability~~	C.2.4.5.1
Infrastructure as a Service	IaaS	• ~~Availability (IaaS Data Center Infrastructure)~~	C.2.5.1.4
Platform as a Service	PaaS	~~• Availability (PaaS)~~	C.2.5.2.4
Software as a Service	SaaS	• ~~Availability (SaaS)~~	C.2.5.3.4
Content Delivery Network Service	CDNS	~~• Availability~~ • ~~GOS (Time to refresh content)~~	C.2.5.4.4
Wireless Service	MWS	• ~~Availability~~	C.2.6.4.1
Commercial Mobile Satellite Service	CMSS	• ~~Availability~~	C.2.7.3
Commercial Fixed Satellite Service	CFSS	~~• Availability~~ ~~• Delay (One Way)~~ ~~• Error Free Seconds (EFS)~~ ~~• Severely Errored Seconds (SES)~~ ~~• Degraded Minutes (DM)~~ • ~~Mean Time to Loss of BCI (MTTLBCI).~~	C.2.7.3
Managed Network Service	MNS	• ~~MNS performance levels will be specified in the TO~~	C.2.8.1.4
Web Conferencing Service	WCS	• ~~Availability~~	C.2.8.2.4
Unified Communications Service	UCS	• ~~Availability~~	C.2.8.3.4

Service	Service ID	~~KPIs Defining the Service-Specific SLA~~	Section C Reference
Managed Trusted Internet Protocol Service – Trusted Internet Connection Portal	MTIPS-TIC	~~• Availability (TIC Portal) – Routine~~ ~~• Grade of Service (Failover Time)~~ ~~• Grade of Service (Monitoring and Correlation) – Routine~~ ~~• Grade of Service (Monitoring and Correlation) – Critical~~ ~~• Grade of Service (Configuration/ Rule Change)~~ ~~• Event Notification (Firewall Security)~~ ~~• Event Notification (Intrusion Detection/ Prevention Security)~~ • ~~Grade of Service (Virus Updates and Bug Fixes)~~	C.2.8.4.4
Managed Trusted Internet Protocol Service – Transport Collection and Distribution	MTIPS	~~• Availability (Port) – Routine~~ ~~• Availability (Port) – Critical~~ ~~• Latency (CONUS) – Routine~~ ~~• Latency (CONUS) – Critical~~ ~~• GOS (Data Delivery Rate) – Routine~~ ~~• GOS (Data Delivery Rate) – Critical~~ • ~~Event Notification (Security Incident Reporting)~~	C.2.8.4.4
Managed Security Service	MSS	~~• Availability~~ ~~• Event Notification~~ ~~• Grade of Service (Configuration Change, Virus Updates)~~ ~~• Incident Response Time (Telephone)~~ • ~~Incident Response Time (On-Site)~~	C.2.8.5.4
Managed Mobility Service	MMS	~~• Event Notification~~ ~~• Grade of Service (Configuration Change)~~ ~~• Incident Response Time (Telephone)~~ • ~~Incident Response Time (Dispatch)~~	C.2.8.6.4
Audio Conferencing Service	ACS	~~• Availability~~ • ~~GOS (Operator Assistance Response Delay)~~	C.2.8.7.4
Video Teleconferencing Service	VTS	~~• Availability~~ • ~~Grade of Service (Completed Service Requests)~~	C.2.8.8.4
DHS Intrusion Prevention Security Service	DIPSS	• ~~Performance metrics for this service shall be defined in the TO~~	C.2.8.9.4

Note: The government considers the above table and all associated references to be its Quality Assurance Surveillance Plan (QASP) in accordance with FAR 46.401.

G.8.2.1.1.2 Service-Specific SLA Credit Formulas

For each failed SLA, the contractor shall apply the associated credit in accordance with Section G.8.4 SLA Credit Management Methodology. The credit shall be calculated

based on the number of times a particular SLA is failed during a rolling six-month window from service acceptance using the following formulas:

- For the first month missing a particular SLA during the six-month window:
  - Service-Specific Credit = 12.5% of the Monthly Charge for a service. This Monthly Charge is either the Monthly Recurring Charge (MRC) for the affected service or the Usage Charge for usage-based services.
- For the second month missing the same SLA during the six-month window:
  - Service-Specific Credit = 25% of the Monthly Charge for the affected service. This Monthly Charge is either the Monthly Recurring Charge (MRC) for the affected service or the Usage Charge for usage-based services.
- For the third (or any subsequent) month missing the same SLA during the six-month window:
  - Service-Specific Credit = 50% of Monthly Charge for the affected service. This Monthly Charge is either the Monthly Recurring Charge (MRC) for the affected service or the Usage Charge for usage based services.
  - The agency may also choose to cancel the affected service without penalty.

G.8.2.1.2 Incident-Based Service SLAs

The Time to Restore (TTR) SLA measures contractor performance on a per-incident basis. The contractor shall calculate the TTR using the following method:

1. Find the elapsed time between the time a service outage is recorded in the trouble ticketing system and the time the service is restored.
2. Subtract time for any scheduled network configuration change or planned maintenance.
3. Subtract time, as agreed to by the government, that the service restoration of the service cannot be worked on due to government-caused delays. Examples of government-caused delays include:
   a) The customer was not available to allow the contractor to access the Service Delivery Point or other customer-controlled space or interface
   b) The customer failed to inform the contractor that a security clearance was required to access the SDP or customer-controlled space
   c) The government required service at a remote site and agreed that a longer transit time was required

For each Incident-based SLA, the contractor shall meet the AQL for the matching KPI associated with the service affected by the incident. The KPIs and associated AQLs for each service are defined in the sections referenced in the table below. Failure to meet

the AQL for an individual incident constitutes failing the SLA for that incident unless due to documented delays caused by the customer.

G.8.2.1.2.1 Incident-Based Service SLA References

Service	Service ID	Section C Reference
Virtual Private Network Service	VPNS	C.2.1.1.4
Ethernet Transport Service	ETS	C.2.1.2.4
Optical Wavelength Service	OWS	C.2.1.3.4
Private Line Service	PLS	C.2.1.4.4
Synchronized Optical Network Service	SONETS	C.2.1.5.4
Dark Fiber Service	DFS	C.2.1.6.4
Internet Protocol Service	IPS	C.2.1.7.4
Internet Protocol Voice Service	IPVS	C.2.2.1.4
Circuit Switched Voice Service	CSVS	C.2.2.2.4
Toll Free Service	TFS	C.2.2.3.4
Circuit Switched Data Service	CSDS	C.2.2.4.4
Contact Center Service	CCS	C.2.3.1.4
Colocated Hosting Service	CHS	C.2.4.5.1
Infrastructure as a Service	IaaS	C.2.5.1.4
Platform as a Service	PaaS	C.2.5.2.4
Software as a Service	SaaS	C.2.5.3.4
Content Delivery Network Service	CDNS	C.2.5.4.4
Wireless Service	MWS	C.2.6.4.1
Managed Network Service	MNS	C.2.8.1.3
Web Conferencing Service	WCS	C.2.8.2.4
Unified Communications Service	UCS	C.2.8.3.4

Service	Service ID	Section C Reference
Managed Trusted Internet Protocol Service – Transport Collection and Distribution	MTIPS	C.2.8.4.4
Managed Security Service	MSS	C.2.8.5.4
Audio Conferencing Service	ACS	C.2.8.7.4
Video Teleconferencing Service	VTS	C.2.8.8.4
DHS Intrusion Prevention Security Service	DIPSS	C.2.8.9.4

G.8.2.1.2.2 Incident-Based Service SLA Credit Formula

For each failed SLA, the contractor shall apply the associated credit in accordance with Section G.8.4 SLA Credit Management Methodology using one of the following formulas based on the nature of the service in question:

- Routine Service Time to Restore (TTR) Credit = 50% of the Monthly Recurring Charge (MRC) for the affected service
- Critical Service Time to Restore (TTR) Credit = 100% of the MRC for the affected service

G.8.2.1.3 Service-Related Labor SLAs

The types of labor services to be delivered will vary widely by TO; as a result, KPIs and SLAs will be specific to and defined in each TO. Similarly, measurement methods, SLA credit formulations, and tracking methodology shall be defined in the TO, see C.2.11 Service-Related Labor for additional information.

G.8.2.2 Service Provisioning SLAs

The SLAs for the provisioning of services under the contract are defined in the subsections below:

- Standard Provisioning SLAs
- ICB Provisioning SLAs
- Project Provisioning SLAs

The provisioning interval for orders shall be measured in days from the TO submission date if no service orders are used, or else from the service order date to the completion date in the SOCN in accordance with Section J.2.4 Ordering:

- Interval = number of days from the service order to the SOCN Completion Date

For associated services ordered together and assigned UBIs with the same service group ID, the SLA shall be governed by the longest provisioning interval.

As described in Section G.3.3.1.3, if the time between the service order and the CWD is greater than the defined provisioning interval for the service as described in the subsections below, the service provisioning SLA is waived for that service on that order.

G.8.2.2.1 Standard Provisioning SLAs

The contractor shall complete orders within the provisioning intervals defined in the table below.

Failure to complete the provisioning of service within the specified timeframes shall constitute a failure to meet the SLA for that provisioning incident.

Note: For orders with non-CONUS delivery locations, these services have individual case basis (ICB) provisioning intervals and follow the requirements described in Section G.8.2.2.2 Individual Case Basis Provisioning SLAs.

G.8.2.2.1.1 Standard Service Provisioning Intervals

Service	Orders SLA (Days)
Disconnect (all services)	30
Circuit Switched Data Service (CSDS)	23
Toll-Free Service (TFS)	45
Private Line Service (PLS):	
PLS ≤ DS1	45
DS1 < PLS ≤ DS3	85
DS3 < PLS ≤ OC3	120
VPN Service (VPNS)	45

G.8.2.2.2 Individual Case Basis Provisioning SLAs

Certain service provisioning tasks do not have predefined provisioning intervals (see the table below for a complete list). For these services, the performance objective shall be defined on an individual case basis (ICB) with the required delivery schedule established in the TO.

Failure to complete the provisioning of service within the timeframe specified in the TO shall constitute a failure to meet the SLA for that provisioning incident.

Notes:

1. For Ethernet Transport Services, see also Section G.8.2.2.4.2 Bandwidth-on-Demand

2. For Cloud Services; including IaaS, PaaS, SaaS, and CDNS; the ICB provisioning interval must be no greater than the provisioning interval proposed as specified in Section G.8.2.2.4

3. For any services proposed under rapid provisioning that also appear on this list, the ICB provisioning intervals must be no greater than the provisioning interval proposed as specified in Section G.8.2.2.4

G.8.2.2.2.1 Services Subject to ICB Provisioning Intervals

Service
• Audio Conferencing Service (ACS) • Cloud Infrastructure as a Service (IaaS) • Cloud Platform as a Service (PaaS) • Cloud Software as a Service (SaaS) • Cloud Content Delivery Network Service (CDNS) • Co-located Hosting Service (CHS) • Commercial Satellite Communications Services (CMSS, CFSS) • Contact Center Service (CCS) • Dark Fiber Service (DFS) • Ethernet Transport Service (ETS) • Internet Protocol Service (IPS) • Managed Network Service (MNS) • Managed Security Service (MSS) • Managed Trusted Internet Protocol Service (MTIPS) • Managed Mobility Service (MMS) • Optical Wavelength Service (OWS) • Unified Communications Service (UCS) • Video Teleconferencing Service (VTS) • Voice Services (IPVS, CSVS) • Web Conferencing Service (WCS)

G.8.2.2.3 Project Provisioning SLAs

For project orders (orders that require special treatment by the contractor due to the size, complexity, or importance of the services ordered), the performance objective shall be based on the baseline completion dates in the Task Order Project Plan (TOPP) agreed upon and documented by the government and the contractor at the time orders are placed and confirmed by the contractor. For these services, the performance

objective shall be defined on an individual case basis (ICB) with the required delivery schedule established in the TO.

Failure to complete the provisioning of service within the timeframes specified in the TOPP shall constitute a failure to meet the SLA. In the event that timeframes are not specified in the TOPP, the standard provisioning SLAs and intervals are defined in Section G.8.2.2 Service Provisioning SLAs.

G.8.2.2.4 Rapidly Provisioned Services

G.8.2.2.4.1 Cloud Service Provisioning

Within the criteria of rapid and elastic provisioning for cloud services as defined by NIST, and as referenced in Section C.2.5 Cloud Service, the contractor shall provide a means of electronically tracking the ordering, confirmation, and provisioning of cloud services such that the intervals between each can be accurately tracked as described in Section G.3.3.3.2 Rapid Provisioning Orders. If the contractor is proposing cloud services, they shall also propose the associated provisioning KPIs and SLAs.

G.8.2.2.4.2 Bandwidth-on-Demand

As described in Section C.2.1.2 Ethernet Transport Services, the contractor shall support bandwidth increments and decrements on demand, as agreed between the contractor and the agency. Unless otherwise agreed by the agency and contractor on a case-by-case basis, provisioning time for this feature shall meet the standard below, measured from the service order to the SOCN.

Service	Provisioning SLA
Ethernet Transport Services: Bandwidth-on-Demand Changes	24 Hours

G.8.2.2.4.3 Other Services Subject to Rapid Provisioning

Consistent with the requirements in Section G.3.3.3.2 Rapid Provisioning Orders, if the contractor is proposing specific services for rapid provisioning, they shall also propose associated KPIs and SLAs.

G.8.2.2.5 Service Provisioning SLA Credit Formulas

For each failed SLA, the contractor shall apply the associated credit in accordance with Section G.8.4 SLA Credit Management Methodology using the following formulas:

- **Default Provisioning Credit** = the larger of:
  - 50% of the Non-Recurring Charge (NRC), or
  - 50% of the Monthly Recurring Charge (MRC).

G.8.2.3 Billing Accuracy SLA

The contractor shall submit accurate billing that meets the performance standards for Billing Accuracy for each TO as defined in Section G.4 Billing. Failure to meet the accuracy standards defined in that section shall constitute failing to meet the Billing Accuracy SLA. If this SLA is failed, the contractor shall apply the associated credit in accordance with Section G.8.4 SLA Credit Management Methodology using the following formula:

- **Billing Accuracy Credit** = 1% of contractor's Total Billed Revenue on the applicable TO for the month.

G.8.3 Service Level General Requirements

The contractor shall be responsible for meeting all SLA requirements as defined in Section G.8.2 Service Level Agreement Tables. This includes delivering the service, maintaining the service at specified AQLs, measuring the KPIs, reporting on compliance, and issuing the specified credit when performance fails to meet the performance objective.

G.8.3.1 Measurement

The contractor shall measure each SLA in accordance with its definition provided in Section G.8.2 Service Level Agreement Tables. Procedures for measuring and sampling shall be described in the quality assurance section of the Program Management Plan, which is described in Section G.9.4 Program Management Plan.

G.8.3.2 Reporting

The contractor shall provide service level management reports as detailed in Section G.8.5 Service Level Reporting Requirements.

G.8.3.3 Credits and Adjustments

In cases where the contractor does not meet the defined contractual or TO SLA, the contractor shall provide credits and/or adjustments to the government agency of record or GSA. This process is further detailed in Section G.8.4 SLA Credit Management Methodology.

G.8.4 SLA Credit Management Methodology

If the contractor fails to meet the performance objectives specified in the SLAs defined above, the government is entitled to receive credit within two billing cycles. The amount of credit shall be calculated as specified in the applicable portion of Section G.8.2 Service Level Agreement Tables.

In cases where multiple SLAs credits are triggered, all credits are paid with the limitation that the total maximum penalty on a service in a given month shall not exceed the total billed cost for that service.

The government may grant a waiver from all or part of a credit if exceptional circumstances warrant.

The TO on the bill defines the customer that will receive the credit and may grant a waiver for all SLAs.

G.8.4.1 Credit Management

The GSA CO, OCO, or authorized ordering official may submit to the contractor an SLA Credit Request (SLACR) as defined in Section J.2.8. In addition, the GSA CO or OCO may designate, in writing, additional personnel or systems authorized to submit SLACRs to the contractor. Additional credit management requirements may be defined in the TO.

The government reserves the right to submit a SLACR at any time within six (6) months of the original SLA failure. For the billing accuracy SLA, defined in Section G.8.2.3, the six-month window for SLACR submission shall begin at the end of the six-month holding period included in the underlying KPI definitions (see Sections G.4.12.1 and G.4.12.2). The contractor shall respond to the request within 30 days by submitting a SLACR response and issue the credit within two billing cycles of this response unless it chooses to reject the request.

The contractor shall work with the government to resolve any disputes and agree on an appropriate credit award in accordance with Section G.4.4 Billing Disputes.

G.8.5 Service Level Reporting Requirements

G.8.5.1 Report Submission

Unless otherwise specified, each report shall be TO-specific and address only those actions and metrics applicable to the TO in question. As specified in Section G.5 Business Support Systems, reports shall be submitted electronically via the contractor's web interface and via direct data exchange.

G.8.5.2 Report Definitions

G.8.5.2.1 Service Level Agreement Report

The Service Level Agreement Report (SLAR) shall document monthly SLA performance covering all aspects of service including incident-based SLAs, service-specific SLAs, and service provisioning SLAs, and billing accuracy SLAs. Report contents are defined in Section J.2.8. The contractor shall deliver this report on the 15th day of each month.

G.8.5.2.2 SLA Credit Request (SLACR) Response

The SLA Credit Request (SLACR) response shall document the contractor's response to a government request for SLA credits (See Section G.8.4.1 Credit Management). Response contents are defined in Section J.2.10. The contractor shall deliver this response within 30 days after the receipt of an SLACR.

G.8.5.2.3 Trouble Management Performance Summary Report

This report shall document trouble management performance by summarizing the number of trouble reports opened and resolved during the reporting period. Unless otherwise specified by the TO, the contractor may use its standard commercial report format for this report provided that it contains the information specified. The contractor shall deliver this report within 14 days after the end of each FY quarter.

G.8.5.2.4 Trouble Management Incident Performance Report

This report shall document trouble management incident-level performance by describing each trouble report issued during the reporting period by contractor trouble report number, agency and AHC, UBI, time opened and time resolved. Unless otherwise specified by the TO, the contractor may use its standard commercial report format for this report provided that it contains the information specified. The contractor shall deliver this report within 14 days after the end of each FY quarter.

G.9 Program Management

This section describes the contractor's requirements for program management, which shall remain in effect through the duration of the contract.

The contractor shall communicate directly with agencies and with GSA. GSA will be accountable for the contractor's technical performance.

G.9.1 Contractor Program Management Functions

The contractor shall effectively and responsively plan, control, and execute against this contract. The contractor shall provide the following program management functions including but not limited to: program control, planning at the program level, planning at the agency level, contractor performance, resource management, revenue management, reporting and reviews, and senior-level communications.

G.9.2 Performance Measurement and Contract Compliance

The contractor's performance shall be measured against the set of SLAs established by the contract. The contractor shall:

1. Submit all SLA data for performance monitoring and reporting to enable an accurate assessment of performance against SLAs as defined in Section G.8.
2. Monitor and manage the contractor's performance against all contract performance requirements.
3. Designate a single interface point for SLA information or issues.
4. Resolve all issues concerning SLAs, including those that pertain to subcontractors. These include, but are not limited to, missing data, data reported in the wrong format or units, late submission from subcontractors, etc.

G.9.3 Coordination and Communication

1. The contractor shall implement consistent and effective communications between management and technical personnel as indicated below in Section G.9.4 Program Management Plan.
2. The contractor shall manage the customer relationship, including, but not limited to:
   a) Government-contractor communications
   b) Resolving trouble reports and complaints
   c) Resolving issue calls
   d) Resolving billing disputes and inquiries
   e) Resolving schedule issues

f) Resolving reporting discrepancies

3. The contractor shall provide technical expertise across all services.
4. The contractor shall answer questions and address issues from the EIS PMO regarding the contractor's network management activities, particularly those that have not been resolved to the government's satisfaction through the standard trouble handling process described in Section G.6.4.1 Trouble Ticket Management General Requirements.
5. The contractor shall provide the escalation procedure for the government to escalate issues to appropriate levels of the contractor's management to resolve disputes and issues.
6. At a minimum, the contractor shall have the capability and authority to:
   a) Support disaster recovery planning and execution
   b) Resolve interoperability problems
   c) Respond to escalation of service concerns
   d) Participate in contract performance reviews
   e) Participate in contract modification negotiations
   f) Perform basic network management functions in support of the government's requirements as described in Section G.8 Service Level Management
   g) Help resolve billing queries and reconciliation issues
   h) Support NS/EP requirements
   i) Provide the EIS PMO with information on customer requirements and customer demographics
7. Within 30 days of the Notice to Proceed, the contractor shall provide and maintain a Contractor Points of Contact List that provides contact information for, at a minimum, the functions that follow:
   a) Provisioning orders
   b) Identifying and resolving service troubles and complaints
   c) Providing customers with status of troubles and resolution
   d) Developing and delivering training
   e) Conducting billing inquiries
   f) Transition project management
   g) Finance
   h) Contracting

i) Account Management (business development and sales)

j) Security

k) NS/EP

8. The contractor shall identify its:

   a) Security POCs who will be processing background investigations and security clearances at the appropriate levels as identified in Section C.1.8.7.7 Personnel Background Investigation Requirements and Section G.5.6 BSS Security Requirements.

   b) POCs that have passed national agency checks or background investigations, and the security clearance levels held by these individuals as defined in Section G.5.6 BSS Security Requirements.

GSA will provide the contractor with contact information (names, phone numbers, and email addresses) for the CO, PM, COR, TSMs and for contacts within the PMO.

G.9.4 Program Management Plan

The contractor shall submit with its proposal a Program Management Plan (PMP) that describes its program management method and implementation plan at a level of detail sufficient to give the government an understanding of the program management approach. The PMP shall address, at a minimum, but is not limited to the following:

1. Summary of contract management requirements, including government dependencies and assumptions regarding government services, facilities, and personnel.
2. Summary Description of the service solution, including the methodologies used to comply with Service Ordering, Billing, Inventory Management, and Service Management requirements.
3. Draft program management schedule.
4. Draft transition management approach. The contractor shall describe its approach to the project management of transition, including the contractor's project management process, procedures, and tools to meet the transition requirements of Section C.3. The Transition section shall address the following areas as well as additional areas proposed by the contractor:

   a) Transition Project Management. The contractor shall address the billing, service ordering, trouble reporting, and customer service processes unique to transitioning onto and off from EIS, specifically including a discussion of how the contractor will expedite transition when it is also the incumbent service provider. The contractor shall describe how it will coordinate with other incumbent providers to ensure a smooth, successful, and timely transition.

The contractor shall identify and assess the major transition risks and propose a response to each.

b) Agency Solicitations. The offeror shall describe its approach to assisting agencies with selecting new or enhanced services to replace services on expiring contracts. The offeror shall identify in the PMP the Transition Management Approach incentives, if any, it will offer agencies to expedite transition.

c) Customer Support during Transition. The contractor shall describe and provide an outline for any transition handbooks or guides it will make available to customers and indicate the target date for publication.

d) Interconnection Plan. The contractor shall describe the interconnection arrangements between the incumbent contractor's network and the EIS networks during the transition, including the interconnection arrangements with the local exchange network, the IXCs, and government private networks. The contractor shall describe any interconnections with other service providers, including other operating units within the contractor's company such as wholesale services, known or expected to be required to transition services and describe the potential impact to customers' operations.

e) Transition Contingency Plan. The contractor shall describe how service will be restored if unforeseen difficulties are encountered at any stage of the transition.

5. Resource plan, providing a management approach to:

   a) Financial Resources: budgeting, tracking, and controlling costs

   b) Human Resources: identifying and retaining qualified personnel and making effective use of their skills

   c) Equipment: managing hardware and software assets

6. Quality Control Program. Management approach to formulating and enforcing work and quality standards, ensuring compliance with contractual SLAs, reviewing work in progress, and providing customer support services.

7. Key Personnel and Organizational Structure . Management structure, organizations, and roles and responsibilities of each function performing work under this contract, key personnel and corporate structure, and subject matter experts as defined in Section H.10 Key Personnel and Corporate Structure .

8. Risk Management. Process for identifying program risks, including risks identified in this contract, and actions to mitigate them.

9. Information Systems. Description of BSS employed to implement the requirements of the contract consistent with security plans to prevent unauthorized access to the government's data and an agency's access to data

belonging to any other agency. Describe how the contractor shall ensure those systems are available to meet the requirements of Section G.5 Business Support Systems

G.9.5 Financial Management

The contractor shall provide a monthly Financial Status Report to the GSA PMO that shows the total dollar activity for the month, broken down by the service types and services in Table B.1.2.1.1, and including the total billed charges for all agencies during the monthly reporting period.

Note: the contractor shall update the list of service types and services with proposals for new or improved services, or when a contract action deletes services from the list.

G.9.6 Program Reviews

G.9.6.1 Quarterly Program Status Reports

The contractor shall deliver Quarterly Program Status Reports to the GSA PMO and lead Quarterly Program Management Review (QPMR) meetings. The Quarterly Program Status Reports shall include, but are not limited to:

- The status of:
  - Project Plan for program management activities
  - Base contract modifications
  - TOs and modifications
  - Projects
  - Orders entered and completed
  - Backlog
  - Aging
  - Pipeline of orders
- Billing disputes
- Summary of trouble reports
- Issues and resolution
- Root cause analysis:
  - Identification of measures failing SLAs
  - Root cause of the failure
  - Corrective action to remedy

- Technical accomplishments and future plans

G.10 Training

The contractor shall provide training on EIS as described below in Section G.10.1 at no additional cost to government customers, as part of the basic service. An agency may request additional (specialized) training as required in a TO. Training shall include courseware development and instructing customer personnel.

The contractor shall include a draft Customer Training Plan in its proposal. The contractor's Customer Training Plan shall detail the designated training for government users that may include the CO and/or CORs, end-users of services, government trainers, and government executives. This training shall remain available throughout the life of the contract. The Customer Training Plan shall list course curricula that educate the government users on the use of the BSS and the performance of tasks related to billing, pricing, order submission and tracking, network performance, trouble ticketing, and inventory management as described below in Section G.10.1. The government reserves the right to provide comments within 30 days of Notice to Proceed. If comments are provided, the contractor shall incorporate them and deliver the revised Training Plan within 15 days after the comments were received.

As mutually agreed by the government and the contractor, training shall be conducted on government premises or contractor premises within daily commuting distance for the government students, or via training methods that include:

1. Instructor-led classroom training
2. Distance learning
3. Online web-based / self-paced learning
4. Interactive video
5. Other remote training methodologies
6. Other methods specified by the government

When training is conducted at a contractor site, the contractor shall provide an appropriate classroom environment and all necessary equipment and support. When training is conducted at a government site, the government will provide the necessary space, equipment, and environmental support. The government may inspect training facilities and may observe training being performed by the contractor to ensure compliance with the contract.

The contractor shall provide training as requested by the government throughout the life of the contract.

G.10.1 Training Curriculum

The contractor shall train designated COs, authorized ordering officials, OCOs, and CORs to fully understand and use the contractor's BSS. The contractor shall provide training that covers the course curriculum (classroom and laboratory, as required) to ensure each student becomes proficient in performing tasks that include, but are not limited to:

1. Use of the contractor's BSS
2. Obtaining price quotes for services and features
3. Ordering services from the contractor via CLINs or ICBs
4. Placing order electronically to add, change, cancel, or disconnect services
5. Adding or changing the features, calling privileges, telephone number or other line attributes that can be changed via "soft" reconfigurations
6. Accepting or rejecting an order or part of an order
7. Reconciling billing
8. Initiating and tracking billing disputes
9. Initiating the inventory management process
10. Initiating and reconciling performance management (SLA) reports
11. Placing and tracking trouble reports for routine and emergency troubles

G.10.2 Training Evaluation

To measure and improve the student's training experience as well as to ensure that the contractor accomplished its purpose, the contractor will provide an automated/online method at the end of each class for the students to evaluate the instructor, effectiveness, course objectives and applicability of the course material, training facilities/method, and offer written comments.

The contractor will be notified by the CO or the OCO in writing of any training that is deemed unacceptable. This notification will identify the unacceptable portion(s) of the training. The contractor shall be responsible for correcting the unacceptable issue(s).

G.11 National Security and Emergency Preparedness

The concept of a national telecommunications infrastructure is recognized in national policy statements and directives issued under the authority of the Executive Office of the President, Congress, the Department of Homeland Security (including the Office of Emergency Communications), and other entities of the government. This telecommunications infrastructure is required to support the critical needs of the government under conditions of stress that range from crises and natural disasters (e.g., flood, earthquake) through declared conditions of National Security and Emergency Preparedness (NS/EP). Public safety and the economic well-being of the nation also depend upon the availability of reliable and responsive telecommunications services. EIS is a key component of the US national telecommunications infrastructure.

NS/EP requirements for telecommunication services are used to maintain a state of readiness or to respond to and manage any event or crisis that causes or could cause injury or harm to the population or damage to or loss of property or that degrades or threatens the NS/EP posture of the United States.

GSA expects to provide assurance for government users that services and other service elements (technical, management, and operations-related) acquired through EIS are in compliance with national policy throughout the life of the contracts. The contractor shall ensure that services delivered are in compliance with national policy directives that apply to the national telecommunications infrastructure. Specific national policy requirements include, but are not limited to, PL 93-288 (Disaster Preparedness Assistance dated May 22, 1974), PPD-1 (Organization of the National Security Council System dated February 13, 2009), PPD-21 (Critical Infrastructure Security and Resilience, dated February 12, 2013), NSDD-97, NSDD-145 and its successors, and other applicable laws, regulations, and directives. Executive Orders (EO) 12472 and 13618 and its successors shall also be considered in the design and operations of services provided under this contract. The contractor shall provide an NS/EP Functional Requirements Implementation Plan with the proposal that addresses the specifications identified in Sections G.11.1–G.11.3, and update it annually.

The contractor shall notify the government immediately when events arise that may have major consequences to its network. This notification is similar to the “abnormal report” currently furnished to the DHS National Coordinating Center (NCC). The GSA CO will set priorities; however, the contractor shall be solely responsible for network operations.

G.11.1 Basic Functional Requirements

For services and CBSAs awarded, the contractor must support the agency's NS/EP requirements which may include the following 14 basic functional requirements for

NS/EP telecommunications and IT services, as identified by the Department of Homeland Security (DHS) Office of Emergency Communications (OEC) (formerly NCS) and the Office of Science and Technology Policy for NS/EP telecommunications services and are now being endorsed by ANSI T1 and ITU-TSS standard bodies and widely supported by contractor communities:

1. Enhanced Priority Treatment. Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic.
2. Secure Networks. Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.
3. Non-Traceability. Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).
4. Restorability. Should a service disruption occur, voice and data services must be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.
5. International Connectivity. Voice and data services must provide access to and egress from international carriers.
6. Interoperability. Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks which will be identified after contract award.
7. Mobility. The ability of voice and data infrastructure to support transportable, re-deployable, or fully mobile voice and data communications.
8. Coverage. Voice and data services must be readily available to support the national security leadership and inter- and intra- agency emergency operations, wherever they are located.
9. Survivability/Endurability. Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.
10. Voice Band Service. The service must provide voice band service in support of presidential communications.
11. Broadband Service. The service must provide broadband service in support of NS/EP missions (e.g., video, imaging, Web access, multimedia).
12. Scalable Bandwidth. NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.

13. Affordability. The service must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).
14. Reliability/Availability. Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence.

G.11.2 Protection of Classified and Sensitive Information

NS/EP related information includes, but is not limited to, databases for classified information; critical users' locations, identifications, authorization codes, and call records; and customer profiles. Additionally, the contractor is provided access to certain classified and sensitive materials required for the planning, management, and operations for NS/EP. That information is in various forms, including hardcopy and electronic media. It will be identified as to its classification and shall be protected by the contractor in accordance with applicable industrial security regulations (National Industrial Security Program Operating Manual [NISPOM] and NSA-approved standards as applicable for Safeguarding Classified Information). The level of classification will be up to and including Top Secret / SCI (Sensitive Compartmented Information), and identified by the government.

G.11.3 Department of Homeland Security Office of Emergency Communications Priority Telecommunications Services

The contractor shall fully comply and interoperate with all Department of Homeland Security (DHS) Office of Emergency Communications (OEC) Priority Telecommunications Services including TSP, Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS) and, when released, Next Generation Network Priority Services (NGN-PS). OEC's Communications Portfolio Management (CPM) Branch collaborates with the public and private sectors to ensure the NS/EP communications community has access to priority telecommunications and restoration services to communicate under all circumstances.

G.11.3.1 Government Emergency Telecommunications Service

Government Emergency Telecommunications Service (GETS) is a White House-directed emergency telephone service provided by the DHS OEC. During emergencies, the public telephone network can experience congestion due to increased call volumes and/or damage to network facilities, hindering the ability of NS/EP personnel to complete calls. GETS provides NS/EP personnel priority access and prioritized processing in the local and long distance segments of the landline networks, greatly increasing the probability of call completion. GETS is intended to be used in an

emergency or crisis situation when the network is congested and the probability of completing a normal call is reduced. GETS is an easy-to-use calling card program; no special phones are required. There is no cost to enroll in GETS, though usage fees may apply. GETS calls will receive priority over normal calls; however, GETS calls do not preempt calls in progress or deny the general public's use of the telephone network. GETS is in a constant state of readiness. It also provides priority calling to most cell phones on major carrier networks. The contractor shall fully comply and interoperate with the GETS service. For more information, see: http://www.dhs.gov/government-emergency-telecommunications-service-gets.

G.11.3.2 Wireless Priority Service

Wireless Priority Service (WPS) is a White House-directed emergency phone service managed by the DHS OEC. WPS complies with the Federal Communications Commission (FCC) Second Report and Order, FCC 00-242, *Establishment of Rules and Requirements for Priority Access Service*.

During emergencies cellular networks can experience congestion due to increased call volumes and/or damage to network facilities, hindering the ability of NS/EP personnel to complete emergency calls. The WPS provides NS/EP personnel priority access and prioritized processing in all nationwide and several regional cellular networks, greatly increasing the probability of call completion. WPS is intended to be used in an emergency or crisis situation when cellular networks are congested and the probability of completing a normal cellular call is reduced. WPS is an easy-to-use, add-on feature subscribed to on a per-cell phone basis. It is deployed by cellular service providers throughout the United States. WPS calls will receive priority over normal cellular calls; however, WPS calls do not preempt calls in progress or deny the general public's use of cellular networks. WPS is in a constant state of readiness. The contractor shall fully comply and interoperate with the WPS service. For more information, see: https://www.dhs.gov/wireless-priority-service-wps.

G.11.3.3 Telecommunication Service Priority

The Telecommunication Service Priority (TSP) System (FCC 88-341) provides a framework for telecommunications services contractors to initiate, restore, or otherwise act on a priority basis to ensure effective NS/EP telecommunication services. The TSP System applies to common carriers, to government, and to private systems that interconnect with commercially provided services or facilities. The TSP System is intended to apply to all aspects of end-to-end NS/EP telecommunication services. The TSP system allows five (5) levels of priorities for restoration (5, 4, 3, 2, or 1) and provisioning (5, 4, 3, 2, 1, or E).

The contractor shall fully comply and interoperate with the TSP system for priority provisioning (i.e., installation of new circuits), restoration of previously provisioned circuits, and priority level for design change of circuits, including coordination between local access providers and the transport segment. The contractor shall fully comply and interoperate with any future TSP replacement system.

Should the contractor's network experience significant degradation or failure, the contractor shall provide priority restoration of affected services in accordance with the TSP system five levels of priorities. In addition, the contractor shall ensure that the restored circuits retain the property of the original circuits (i.e., TSP levels). [Note that the contractor is only obligated for priority restoration and provisioning of those circuits that agencies have obtained TSP priorities from EOC.

TSP Authorization Codes are active for three (3) years, at which point the service user will need to revalidate them. Service users must request TSP restoration priority **before** a service outage occurs.

G.12 Requirements for Climate Change Adaptation, Sustainability and Green Initiatives

G.12.1 Climate Change Adaptation

EIS seeks to benefit from the use of sustainable management practices by contractors including tracking and seeking continual reductions in energy usage, greenhouse gas (GHG) emissions, water consumption, solid waste and hazardous waste, and other relevant environmental impacts and associated costs. Use of sustainable management practices results in lower environmental impacts of delivered products and services, helping customers meet the GHG emissions reduction, sustainable acquisition, and climate change adaptation requirements under Executive Order 13693, – Planning for Federal Sustainability in the Next Decade, and its precursors, successors and related regulations and guidance.

Public disclosures of environmental impacts and sustainable management practices have been associated with reduced supply chain and other business risks for disclosing companies. Sustainability disclosures can help EIS customers understand the major environmental impacts of procured products and services, familiarize themselves with the available strategies for reducing these impacts, and design projects and TO requirements which incorporate these strategies.

GSA will require corporate sustainability reporting. GSA encourages the contractor to provide the location(s) (Internet URL or URLs) of one or more sources of publicly available information regarding company-wide environmental impacts and sustainable management practices (sustainability disclosures) on the contractor's EIS webpage. In making sustainability disclosures, the contractor is requested to use existing, widely recognized third-party sustainability reporting portals and services such as the Global Reporting Initiative (GRI) Sustainability Disclosure Database (database of corporate social responsibility (CSR) reports) and the Carbon Disclosure Project (CDP) Climate Change and Water Disclosure Questionnaires. All sustainability disclosures shall be kept up-to-date and accurate.

These sustainability-related standards, including estimates of the lifecycle costs and environmental impacts of proposed solutions, shall apply at the TO level.

GSA has a leading role in ensuring that the federal government is better prepared to cope with the consequences of climate change adaptation that presents many serious risks for government operations. These risks include damage to facilities and equipment, and disruptions to communications networks and transportation routes needed to deliver supplies and services. Climate change adaptation aspects shall be considered in the design and operations of services to be provided under this contract.

The contractor shall incorporate climate change adaptation strategies into risk-management programs to reduce property, infrastructure, and supply chain vulnerabilities. This includes identifying mission critical facilities, products and services, evaluating business operations and supply chains that may be vulnerable and anticipating needs that may arise from climate change. The contractor shall comply with the climate change adaptation conditions described in Executive Order 13693, – Planning for Federal Sustainability in the Next Decade, and other applicable laws, regulations, and directives.

Executive Order 13693 – Planning for Federal Sustainability in the Next Decade, requires agencies "To improve environmental performance and Federal sustainability, priority should first be placed on reducing energy use and cost, then on finding renewable or alternative energy solutions. Pursuing clean sources of energy will improve energy and water security, while ensuring that Federal facilities will continue to meet mission requirements and lead by example. Employing this strategy for the next decade calls for expanded and updated Federal environmental performance goals with a clear overarching objective of reducing greenhouse gas emissions across Federal operations and the Federal supply chain." In support of this requirement, contract awardees shall prepare and update as needed Corporate Climate Risk Management Plans that will be made available for agency use to directly support the Agency Adaptation Plans of agencies procuring services through this contract.

Contractors shall conduct corporate sustainability reporting through accredited third parties and provide copies of their reporting to GSA.

The contractor shall deliver a yearly Climate Change Adaptation, Sustainability, and Green Initiatives Report to the GSA CO that highlights any changes made throughout the year to remain fully compliant with the federal directives mentioned above. Section F contains the schedule for all contractual deliverables.

The contractor shall notify the agency and the GSA CO immediately if conditions arise thought to be out of compliance with the aforementioned Executive Orders, laws, regulations, and directives.

G.12.2 Sustainability and Green Initiatives

GSA is committed to environmentally friendly sustainable practices that reduce the federal government's environmental footprint. The contractor shall provide sustainable products and services whenever possible. Both the sustainable acquisition and data center requirements of Executive Order 13693 – Planning for Federal Sustainability in the Next Decade shall be considered in the design and operations of services to be provided under this contract. The contractor shall comply with the climate change

adaptation conditions described in the aforementioned Executive Orders, and other applicable laws, regulations, and directives.

The contractor shall notify the agency and GSA COR immediately if conditions arise thought to be out of compliance with the aforementioned Executive Orders, laws, regulations, and directives.

Commercially available products under this contract may be covered by the Energy Star®, Federal Energy Management Program (FEMP), or Electronic Product Environmental Assessment Tool (EPEAT) programs. For applicable products, the contractor is encouraged to offer Energy Star-qualified/certified products, products meeting FEMP low-standby power levels, and EPEAT-registered products, at the Bronze level or higher. If the contractor opts to offer Energy Star-certified, low standby power, or EPEAT-registered products then they shall identify by model which products offered are Energy Star-qualified/certified, meet FEMP low standby power levels, and/or EPEAT-registered, with EPEAT-registered products broken out by registration level of bronze, silver, or gold. Visit the Green Procurement Compilation at www.sftool.gov/greenprocurement for a complete list of products covered by these programs.

E.O. 13693 requires agencies to improve data center energy efficiency at federal facilities. The E.O. Implementing Instructions encourage agencies to use data center shared service providers and contracted data center services, including cloud services, which are provided through data centers that meet power utilization efficiency targets between 1.2 and 1.4.

G.12.2.1 Electronic Product Environmental Assessment Tool

Under this contract, the contractor shall deliver, furnish for government use, or furnish for contractor use at a federally-controlled facility, equipment that was EPEAT bronze-registered at the bronze level or higher throughout the life of the contract.

The contractor shall deliver a yearly Climate Change Adaptation, Sustainability, and Green Initiatives Report to the GSA CO that highlights any changes made throughout the year to remain fully compliant with the federal directives mentioned above. Section F contains the schedule for all contractual deliverables.

G.12.2.2 Energy Efficient Products

The contractor shall ensure that energy-consuming products are energy efficient (e.g., Energy Star-certified products or Federal Energy Management Program (FEMP)-designated products or low standby power products) throughout the life of the contract, in compliance with FAR Clause 52.223-15 Energy Efficiency in Energy-Consuming Products.

G.12.2.3 Data Centers and Cloud Services

The contractor shall identify which data center or cloud services, if any, will be provided through data centers meeting power utilization efficiencies (PUE) between 1.2 and 1.4. The contractor shall report annually the PUE of data centers used under this contract.

Enterprise Infrastructure Solutions (EIS)
Request for Proposals

Section H
Special Contract Requirements

Issued by:

General Services Administration

Office of Integrated Technology Services

(b) (2) [redacted]

[redacted]

JULY 2017

Table of Contents

H.1 Type and Term of Contract

This contract is an indefinite delivery, indefinite quantity, fixed price and time and materials contract with a form of economic price adjustment.

The term of this contract will be five years from the effective date of award with two (2) five-year government options to extend. The total term of the contract will not exceed 15 years and 9 months.

H.2 Order Types

As defined in FAR Part 16, Type of Contracts, all types of Fixed-Price and Time and Materials (T&M) are permissible for orders under the contract.

Indefinite Delivery, Indefinite Quantity, Blanket Purchase Agreements, and Letter Contracts are not permissible order types under the contract.

Orders may be multi-year and/or include options as defined in FAR Part 17 and agency-specific FAR Part 17 supplements.

H.3 Authorized Users

a) This contract is for the use of all Federal agencies; authorized Federal contractors; agency-sponsored universities and laboratories; and when authorized by law or regulation, state, local, and tribal governments, and other organizations. All organizations listed in General Services Administration (GSA) Order OGP 4800.2I (as updated) are eligible

b) The government has the right to add authorized users as defined in paragraph a) at any time during the term of this contract up to the limits specified in Section H.4 - MINIMUM REVENUE GUARANTEE AND MAXIMUM CONTRACT LIMITATION.

c) The government is not obligated nor required to use this contract to satisfy its requirements for the services described.

H.4 Minimum Revenue Guarantee and Maximum Contract Limitation

a) The minimum revenue for the EIS program is $75 million per awardee.

b) The maximum all-inclusive funding ceiling for this and any other contracts awarded as a result of RFP #QTA0015THA3003 is $50 billion.

c) After award, the government will not manage or assign traffic or service to maintain a predetermined revenue share to the contracts, if there are multiple awardees.

d) The government, at the government's option, may satisfy the Minimum Revenue Guarantee by using and paying for the contractor's services provided under the

contract or by direct payment(s) to the contractor, or by any combination of use and payment of the contractor's services and direct payment(s) to the contractor.

H.5 Disclosure of Information

a) Any government information made available to the contractor shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract.

b) In performance of this contract, the contractor agrees to assume responsibility for protecting the confidentiality of government records and for ensuring that all work is performed under the supervision of the contractor.

c) Each officer or employee of the contractor, its subcontractors and agents, to whom information may be made available or disclosed shall be notified in writing by the contractor that information disclosed to such officer or employee shall be used only for a purpose and to the extent authorized herein. Use of such information for a purpose or to an extent unauthorized herein may subject the offender to criminal sanctions imposed by 18 U.S.C. 641. The law provides, in pertinent part, that whoever knowingly converts to their use or the use of another, or without authority sells, conveys, or disposes of any record of the United States or whoever receives the same with intent to convert it to their use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine of up to $10,000, or imprisonment up to ten years, or both.

H.6 Reserved

Reserved

H.7 Price Management Mechanism

The Price Management Mechanism (PMM) ensures that EIS prices remain at or below the best commercial prices in the industry for large commercial and government customers. The purpose of this clause is to describe the overall process to be followed to achieve this result.

All services on the contract are subject to the PMM.

For a given service, the government may implement the PMM process any time it deems there is a divergence between the EIS pricing and comparable commercial and government prices. However, the PMM will not be implemented more than twice for a given service in any given 5-year contract period for a maximum of six times during the planned 15-year life of this contract. The first PMM implementation will not take place until at least 12 months after contract award.

H.7.1 PMM Process

After contract award, the government will continuously use available information to compare contractor EIS prices with competitive prices offered to commercial and government users. Comparison prices will be acquired from (1) the commercial websites of EIS contractors, (2) Federal and State tariffs, (3) other government contracts including the Multiple Award Schedules, (4) publicly available price-change indices, and/or (5) any other sources determined by the government to be relevant for price comparison purposes. If the government determines that contractor prices are not consistent with the comparison prices, or if the government has insufficient information to make a price comparison, the government at its sole discretion will select specific services for PMM analysis. The government will then proceed to Phase One of the PMM process. There is no requirement for the government to share its analyses with the contractor or provide a justification for its determination to proceed to Phase One.

H.7.2 PMM Phase One

In Phase One, the government will identify those services that it has determined should be reduced in price, and will provide a detailed request for a specific price reduction approach from the contractor for each service identified.

The contractor shall respond in writing to the government request within 60 days. The response shall include one of the three following responses:

1. Agreement that the requested price reduction is warranted, along with a proposed approach to realizing the requested reduction based on specific price reductions for specific services and CLINs.
2. Agreement that some price reduction is warranted, along with a counter-proposal for reduction and a detailed approach to realizing the proposed reduction based on specific price reductions for specific services and CLINs.
3. Disagreement that any price reduction is warranted along with documented justification for this position.

If option one or two is selected, the government will verify the details of the proposal. If the proposal is satisfactory, the PMM process is concluded.

If not, then the government will provide the basis for its position regarding the insufficiencies of the proposal. Discussions shall continue in good faith until either (1) the parties agree, at which point the PMM is concluded, or (2) the parties continue to disagree. If the parties cannot agree on a satisfactory adjustment process, then the process shall proceed to Phase 2.

If option 3 is selected then the process shall continue to Phase 2.

H.7.3 PMM Phase 2

Under Phase 2, the contractor shall provide comparison contracts to the government for further analysis of the contractor's specific market pricing for comparable customers. The contractor shall provide these contracts immediately as part of its response under the third option in H.7.2.3 above. Alternatively, if the parties have not been able to agree on a suitable reduction under option 2, above, then the contractor shall provide these contracts within 30 days of notice by the government that the process has stalled, and is moving to Phase 2.

The contractor shall provide multi-service and single-service comparison contracts in accordance with the following procedures.

For each service identified by the government, the contractor shall deliver its three largest multi-service contracts that contain the service selected by the government for PMM analysis. The contract size of a multi-service comparison contract is defined as the total dollar figure billed to that contract's customer for all services for the most recent three full months (from the time of the government's request for contract submissions).

The contractor shall submit the three largest multi-service contracts that contain the service. The contractor shall additionally submit from one to three single-service contracts (single-service contracts contain only the service under evaluation) in accordance with the procedures in the following paragraph.

The single-service contract submission selection shall be based on the contract size, where single-service contract size is defined as the total dollar figure billed to a contract's customer for the most recent three full months (from the time of the government's request for contract submissions). The contractor shall, at a minimum, submit the largest sized single-service contracts for the same service over the same three months.

Government contracts that satisfy the submission requirements above shall be included in the submissions but shall be limited to no more than one multi-service and one single service contract per service. The EIS contract and Multiple Award Schedules (MAS) shall not be considered in the selection or submission of comparison contracts. All other submission requirements shall be met with commercial contracts. The contractor shall also deliver to the government the access line prices with all rate affecting terms for each contract submission.

Using these procedures, the contractor shall provide a minimum of three and a maximum of six comparison contracts for each service.

Comparison contracts that are sales of (1) promotional offerings where the service ordering by the contract customer is limited to one month or less, or (2) service, such as

to equity partners and other carriers, that are absent of typical customer terms (e.g., detailed billing and full-service account management), or (3) contracts where the limited geographic availability of service was a significant factor in the pricing of the service offered, or (4) contracts exhibiting extreme internal price imbalances will not be eligible for use in the PMM process.

Any assertion that a contract is not appropriate for use as a comparison contract under the above provisions must be made to the CO upon delivery of the comparison contracts. The CO will make the determination of which contracts will not be eligible for use under provisions (1) to (4) above. If a contract is excluded, the government reserves the right to request a replacement contract(s).

Additionally, at the government's request, the contractor shall supply the replacement of a comparison contract in cases where it does not contain sufficient price elements to match the EIS service traffic. The replacement(s) of the rejected contract(s) shall be selected in accordance with the requirements listed above. For example, a contract submission that offers only T1 private line prices would be unsuitable for a PLS comparison if the EIS service traffic had a significant number of circuits at other speeds.

The multi-service and single-service comparison contracts shall be drawn from contractor's customer contracts. The contract comparison submission information provided by the contractor shall include all rates, prices that are referenced in other offerings, and rate affecting terms and conditions that are required to implement the PMM for that service. The contractor shall clarify contract submission language or provide missing contract data within 5 business days at the government's request.

If any of the submitted contract comparison data is publicly available, e.g., on the contractor's website or in tariffs, the contractor shall additionally provide references to find such information. In addition to the contract submissions and public references, the contractor shall provide its understanding of how the prices are to be applied to the EIS service traffic in the form of price tables, including applicable discounts, waivers, and credits. The deliverables shall be in electronic form.

Contractor compliance with the submission information requirements of the PMM shall be certified in writing by an employee of the company who has the authority to bind the company. If the contractor fails to comply with the contract submission requirements of this section, the government reserves the right to use comparison prices from any sources it deems appropriate to substitute for the contractor's contract comparison submissions.

The government will analyze the submitted comparison contract information, and if the government continues to believe that the contractor's EIS prices for a service(s) are not

competitive with the prices in the contract submissions, the government will proceed to Phase 3. Otherwise, the PMM process is concluded.

H.7.4 PMM Phase 3

During Phase 3, the government will assess the service by comparing the contractor's EIS prices for the service to the contractor's submitted comparison prices for that service. To make a comparison, the government will develop a statistically significant demand set (called PMM demand set) from the contractor's EIS network demand (including network usage, circuits, ports, EVCs, and/or other components that determine the price for services) and use it to compare prices.

Total prices for each service are calculated by multiplying the EIS or comparison contract unit prices by the PMM demand set and applying other price affecting terms, such as discounts, waivers, and credits. Access line prices, but not Service Related Equipment (SRE) prices, will be included in the calculation.

The EIS price calculation totals for each PMM demand set will use EIS unit prices that will be in effect during the period following the PMM evaluation process. At its discretion, the government may perform separate PMM calculations and price reduction determinations within a service for communications between: CONUS and CONUS; OCONUS location(s) and CONUS or OCONUS; and/or Country/Jurisdiction(s) and any location.

There will be one EIS total price calculation and three to six comparison contract price total calculations (a total price calculation for each submitted comparison contract) for each service. The number of total price calculations for a service may increase if the government decides to perform separate calculations for communications between: CONUS and CONUS; OCONUS location(s) and CONUS or OCONUS; and/or Country/Jurisdiction(s) and any location. If the government decides to use these separate calculations for a service, the collection of these separate calculations (and any related price reductions) shall count as only one of the six PMM implementations over the life of the contract.

For submitted multi-service contracts, a calculated comparison total price will be computed only for the service(s) under PMM consideration. For submitted single-service contracts, a comparison cost will be computed for the single service only.

For each service, the final comparison total price is calculated by averaging the two lowest total prices from the comparison contracts. The resulting average total price from the comparison contracts will be compared with the total price calculated from the contractor's EIS total price for the service. If the total EIS calculated price is at least five percent greater than the calculated average comparison price total for a service, a price

reduction will be required by the contractor as specified in Section H.7.5. Otherwise, if the total EIS calculated price total is not at least five percent greater than the calculated average comparison price total, the PMM process is concluded.

H.7.5 Basis for Phase 3 Price Reduction Request

Phase 3 price reductions will be requested based on calculation results using comparison prices submitted by the contractor as explained above. If the total EIS calculated price is at least five percent greater than the calculated average comparison price total for a service, the government will require a price reduction. Accordingly, the contractor shall reduce its EIS contract unit prices so that the calculation of the PMM demand set using these reduced unit prices shall yield a total price equal to or below the final comparison total price as described in H.7.4. The contractor has the discretion to select which contract unit prices in the service to reduce that achieve the required service price reduction. The contractor shall not increase any EIS contract unit prices when implementing a PMM price reduction.

The government will provide the contractor the calculation assumptions, unit prices, demand sets, and pricing model access (but not source code) so that the contractor can confirm the government's calculation results and to assist the contractor in selecting which EIS unit prices to reduce. The government and contractor shall enter discussions, at the contractor's request, to clarify assumptions, correct errors, and/or address other issues related to the calculations.

The contractor shall submit the price tables to the government that reflect the price reduction in a contract modification proposal within 30 days after receiving the written request for a price reduction from the CO. The price reduction shall become effective beginning with the third billing period or within 90 days, whichever is less, after the effective date of the modification. The unit price reductions shall be effective for the remainder of the period in effect unless replaced as allowed by the contract and its modifications.

H.7.6 Alternate Dispute Resolution Process

If the contractor disagrees with the price reduction within 30 days of the contractor's receipt of a written request to reduce prices from the CO, the contractor shall issue a "Notice of Disagreement." If the parties are still unable to agree to a price reduction within 15 days after issuance of the "Notice of Disagreement" then the following will apply. The parties shall agree upon an Alternative Dispute Resolution (ADR) process that will resolve the dispute within 90 business days after submittal in accordance with ADR Techniques as described in GSA publication CSL P 5050.1A. If the parties are unable to resolve the dispute using this ADR process, the contractor may file a claim pursuant to FAR 52.233-1 Disputes.

H.8 Price Reductions

a) The contractor may offer additional discounts on orders with no change to the contract pricing.

b) Subsequent price reductions on the contract shall reduce prices prospectively on all awarded task orders from the effective date of the contract price reduction modification. Such price reductions do not apply to prices that have been differentiated on a task order and have been associated with an agency task order number in the Section B table.

c) The contractor may reduce contract prices at any time. Price reductions other than those implemented by the government under the Price Management Mechanism (PMM) (H.7) and Economic Price Adjustment – Price Refreshment (H.19) clauses of this contract, or covered by subsection (a) above, shall be subject to the following conditions:

   1. The contractor shall propose all price reductions to the GSA CO as a contract modification.
   2. The proposed price reduction shall be effective on the first day of a given month.
   3. The proposed price reduction shall be applicable to all agencies.
   4. Price reduction proposals shall include all contract pricing tables, and the effective date(s) of the price reduction. The contractor shall provide all revised pricing tables in an electronic format.
   5. Should the government execute a price reduction modification on a date after the proposed price reduction effective date, in accordance with subsection (c) (2) above, the price reduction shall be deemed to have occurred on the first day of the next month for that service or if the price reduction is to be retroactive, as mutually agreed to by the government and the contractor.

H.9 Electronic Access to Contract

Within 30 calendar days of award, the contractor shall post its redacted contract to its public website. The redacted version shall be provided to the CO within seven days if requested. The contractor shall prepare the proposed redacted version in accordance with Freedom of Information Act. All government location information and addresses shall be redacted for security purposes. Proposed redacted modifications shall be posted no later than the 12th calendar day of each month to reflect all contract modifications of the previous month. The redacted version of any and all modifications shall be provided to the CO within seven (7) days if requested. The GSA CO is the final approval authority for redactions. As necessary, the contractor shall correct and repost redactions at no additional cost to the government.

All modifications shall be incorporated electronically in context within the contract in accordance with the “Guidelines for Modifications to EIS Program Contracts” in Attachment J.4.

H.10 Key Personnel and Organizational Structure

H.10.1 Key Personnel

The contractor shall identify individual(s) by name selected to fill the following contractor key personnel roles in its proposal:

a) EIS Program Manager.

The contractor shall provide information to include, but not be limited to:

a) Responsibilities.

b) Voice telephone number.

c) Cell telephone number (if used).

d) E-mail address.

The contractor may submit the information listed above for other personnel it considers important to the overall operation and success of the contract.

H.10.2 Substitutions and Additions of Contractor Key Personnel

The following instructions address the procedures for substitution of key personnel defined in Section H.10.1:

a) Resumes for substitutions and/or additions to the contractor’s key personnel under this contract shall be submitted for the written approval of the GSA CO. Any substitutions and/or additions shall be subject to the terms and conditions of this requirement.

b) During the first 180 days of contract performance, no key personnel substitutions shall be permitted unless such substitutions are due to illness, injury, death, disciplinary action, demotion, bona-fide promotion, termination of employment, or other exceptional circumstances when approved by the GSA CO. In any of these events, the contractor shall promptly notify the GSA CO and provide the information required by paragraph c) below. After the initial 180-day period, in accordance with paragraph c) below, all proposed substitutions and additions of key personnel shall be submitted to the GSA CO in writing 15 days (30 days if security clearance is to be obtained) prior to the contractor anticipated effective date of the proposed substitutions and additions.

c) For all requests for substitutions and additions, the contractor shall provide a detailed explanation of the circumstances requiring the proposed substitution or addition. A complete resume for each proposed substitute or addition, and any other information requested by the GSA CO shall be provided. The contractor shall certify that the proposed replacement is better qualified than, or at least equal to, the key personnel to be replaced, subject to the penalties in 18 USC 1001. The GSA CO or the GSA CO's authorized representative will evaluate such requests and promptly notify the contractor of the approval or disapproval thereof.

H.10.3 Organizational Structure

The contractor shall submit its organizational structure (e.g., org chart) in its proposal, and shall update its organizational structure throughout the life of the contract. Updates shall be provided within 30 days of any change to the contractor's organizational structure.

This documentation shall include, but not be limited to, the following information:

a) Charts that show the functional relationships among organizational elements and identify the positions of key personnel assigned to carry out this contract.

b) Relationship of the highest ranking individual assigned to this contract to the corporate Chief Operations Officer, President, and Chief Executive Officer.

c) Organization charts and plans that clearly depict the areas of responsibility and flow or authority between the contractor and its subsidiaries and/or major subcontractors.

d) Charts and descriptive text indicating the contractual, technical, and administrative interfaces between the government and the contractor, the contractor's subsidiaries, and major subcontractors.

e) A description of corporate escalation procedures for resolving critical issues, including points of contact.

H.11 Protection of Proposal and Contract Information

In accordance with Federal Acquisition Regulation (FAR) Part 3.104-4, the government will take the necessary and usual steps to maintain the confidentiality of information submitted prior to award of the contract and contract modifications. Although Section H.9, Electronic Access to Contract, advises the contractor of Freedom of Information Act redaction, the contractor is advised that the government will make all current year unit contract prices publicly available.

H.12 Reserved

H.13 Other Government Contractors

Under the EIS program the government may award several contracts to provide various forms of technical and management services. Government agencies may also use support contractors to assist them with the EIS contract. Once these contractors are operating in their official capacity as agents for the government, the contractor shall provide them full cooperation, including but not limited to, full access to relevant portions of the EIS contracts, all requested reports, data, and other information regarding the government's service. These support contractors will complete the Certification for Nondisclosure of Information and Conflict of Interest forms. The GSA CO is the sole approving authority for these forms.

H.14 Taxes

The government generally will pay all allowable Federal, state and local taxes applicable to telecommunications services delivered under this contract in accordance with FAR Clause 52.229-4, with the following exceptions:

- Taxes from which the Federal Government is expressly exempt under the authorizing state statute or local ordinance.
- Any state or local tax whose legal incidence is on the Federal Government.

The CLIN prices for services and features (as defined in the Section B pricing tables) shall not include domestic Federal, state, or local taxes, or non-domestic taxes and duties in effect that the taxing authority is imposing and collecting on the transactions or property covered by this contract. Excepted taxes, as defined in Federal Acquisition Regulation (FAR) 52.229-4, shall be included in the CLIN price. Non-excepted Federal, state and local taxes shall be billed separately from the CLIN prices (see Agency Request for Fully Loaded CLIN Prices for opposite treatment).

Special attention must be paid to the treatment of the Associated Government Fee (AGF), which will be included in the prices of services as explained in Section J.2.10. The contractor shall not include Federal, state and local taxes in its AGF calculation when Federal, state and local taxes are billed separately from the CLIN price (see Agency Request for Fully Loaded CLIN Prices for opposite treatment). For example, the contractor shall not include the AGF when calculating the EIS revenues to which a state or local tax applies. The exclusion of the AGF is for the purposes of tax calculations only; for all other billing purposes the AGF shall be handled in accordance with the billing processes.

GSA will provide the contractor with a file of all taxes that have been previously deemed allowable by GSA. Any tax included in the file may be invoiced by a contractor in accordance with the following:

- The tax is applicable to the service in question.
- The tax is invoiced at the proper rate.
- The invoice includes the tax citation from the file.

If a contractor needs to invoice a tax that is not in the file, the contractor must provide the following 30 days prior to including the tax in question on an invoice:

- The name of each tax.
- The jurisdiction by name.
- The statutory source (include web reference if possible) for the tax.
- The applicable tax rate(s).

The CO shall notify the contractor within 30 days after receipt of the information above as to whether or not the tax is allowable under the terms and conditions of the contract. If the tax is deemed allowable, it will be added to the file within 15 days.

The contractor and the government shall follow the same process outlined above when notifying the CO of "after-imposed taxes" as defined in FAR Clause 52.229-4.

The contractor shall provide to the government, on a semi-annual basis, an itemized list of taxes that are included in its monthly invoices, including the name of each tax, jurisdiction by name, reference to the statutory source for the tax, and applicable tax rates. See Section F for the specific deliverable.

Agency Request for Fully Loaded CLIN Prices

A direct billed agency may elect, at its discretion, to request that all taxes be included in the CLIN prices proposed in response to an agency task order solicitation. For any task order requiring that all taxes be included in the CLIN prices, the ordering agency will be responsible for ensuring that only applicable and allowable taxes have been assessed and included in the CLIN prices. The AGF shall be assessed on the fully loaded CLIN prices under this option.

H.15 Press Releases

Press releases pertaining to this contract shall not be made without prior approval of the CO. A minimum of three business days' notice is required for approval.

H.16 Permits

The contractor shall, without additional expense to the government, be responsible for obtaining any necessary licenses, certifications, authorizations, approvals, and permits, and for complying with any applicable Federal, state, and municipal laws, codes, and regulation, and any applicable foreign work permits, authorizations, etc., and/or visas in connection with the performance of the contract, whether domestic or non-domestic.

H.17 Contractor-Provided Equipment

The government reserves the right to acquire ownership of contractor-provided Service Related Equipment (SRE) installed pursuant to the provisions in Section B.2.10, at any time during the contract period. This option to acquire ownership shall be consistent with the provisions of FAR 52.207-5. The purchase conversion cost for SRE acquired by the government shall be the paid SRE NRC or the sum of SRE MRC payments for the full SRE MRC term.

If an authorized user initially elects an SRE MRC payment term and subsequently chooses to assume ownership prior to the completion of the SRE MRC payment term, the user shall be permitted to pay the SRE NRC for the SRE minus the value of all SRE MRC payments paid up to the time that the user assumes ownership, with such SRE MRC payment amounts reduced to remove that portion of the payments reflecting the adjustment for the Monthly Payment Factor. No charges will be incurred by the government as a result of any changes to User-to-Network Interfaces (UNIs) (i.e., replacement of one UNI by another UNI) resulting from the transfer of ownership. Any manufacturer's warranty remaining on SRE, at time of title transfer, will transfer to the government; to the extent such warranty transfer is permitted by the terms of the manufacturer's initial warranty. However, where maintenance of the SRE continues after the title transfer, pursuant to the provisions in Section B.2.10, the contractor providing such maintenance will manage the warranty on the SRE for the government and will receive such monetary benefits as might result from operation of the warranty.

H.18 End of Life

The contractor shall provide all services awarded for the duration of the contract. This includes services awarded at contract inception and those added during the life of the contract by modification. If the contractor determines that any of these services can no longer be supported due to obsolescence, the contractor shall notify the GSA CO in writing of plans to withdraw the service at least eighteen (18) months prior to the proposed date of the withdrawal. At that time, the contractor must propose to the government an acceptable plan to ensure service continuity and transition to new services. The GSA CO must approve any withdrawal of service offerings through a

contract modification. GSA approval will not be unreasonably withheld if the contractors' continuity plan for transitioning existing users to new services is acceptable to the Government.

The contractor may submit a proposal after approval of its withdrawal notice to increase the prices for the end of life (EOL) services. The proposed price increase will be negotiated with the GSA CO. All task orders will also require a modification to reflect the price increase.

H.19 Economic Price Adjustment – Price Refreshment

The government intends to conduct price refreshment prior to the exercise of each contract option period. The price refreshment may result in price increases or price decreases and will be conducted in accordance with the following process:

a) The contractor shall submit revised prices for Option Period 1 or Option Period 2 for existing price tables five (5) months prior to the award date of the first or second option period. Revised prices shall not exceed the economically adjusted prices (EAP) to be determined as described below. Revised prices may be less than the EAP prices at the contractor's discretion.

b) Price adjustments will be effective on the first day of the following option period.

c) EAP prices shall be determined utilizing the following market indicators:

   1. Annual Cost Employment Index: The Bureau of Labor Statistics (BLS) publishes annual Employment Cost Index (ECI) for private industry workers (Employment Cost Index for total compensation, for private industry workers, by occupation and industry (not seasonally adjusted)) that shall be used to determine escalation factors for hourly labor rates on this contract (http://www.bls.gov/ncs/ect/).
   2. Annual Producer Price Index for Wireline Telecommunication Carriers NAICS 517110 will be used for all services. (http://www.bls.gov/ppi/).

d) Services and labor under this contract are mapped to the following indices:

   1. Labor – Table B.2.11.7.2 Service Related Labor Pricing Instructions Table includes the Occupational Group category which determines the specific ECI indices to be utilized.
   2. Services:
      i. The following services shall utilize the PPI for Wireline Telecommunication Carriers 517110:
         A. Data Service
         B. Voice
         C. Contact Center Service
         D. Data Center Service

E. Cloud Service
F. Managed Service
G. Cable and Wiring
H. Access Arrangements
I. Mobile Wireless Service
J. Satellite Service

e) EAP Price determination:

NOTE: The EAP price calculation shall be completed by the contractor using the spreadsheet provided in Section J.15. The procedure below is intended only to document the calculation performed by the spreadsheet. The contractor shall enter the contract award date in the CONFIG tab in the aforementioned spreadsheet prior to completing the following.

In performing the EAP price calculations, the following definitions shall be observed:

- **Start Index**: For Option Period 1 price calculations, the **Start Index** shall be the value of the applicable index given in paragraph c) above, with the index published date closest to the Relative Dates Row of the Rates tab of the aforementioned spreadsheet in Section J.15.
- For Option Period 2 price calculations, the **Start Index** shall be the value of the applicable index given in paragraph c) above, with the index published date closest to the Relative Dates Row of the Rates tab of the aforementioned spreadsheet in Section J.15.
- **End Index**: For Option Period 1 price calculations, the **End Index** shall be the value of the applicable index given in paragraph c) above, with the index published date closest to the Relative Dates Row of the Rates tab of the aforementioned spreadsheet in Section J.15.
- For Option Period 2 price calculations, the **End Index** shall be the value of the applicable index given in paragraph c) above, with the index published date closest to the Relative Dates Row of the Rates tab of the aforementioned spreadsheet in Section J.15.

The following rounding conventions shall also be observed:

- In all steps, results shall be rounded to the nearest hundredth, rounding up from 5. As examples, 78.2367 shall be rounded to 78.24, and 78.235 shall also be rounded to 78.24.

The following procedure shall be used for Option Period 1:

1. Determine the escalation rate over (4) (12) month periods by dividing the value of the Option Period 1 **End Index** by the value of the Option Period 1 **Start Index**:

$$\text{Escalation over (4) (12) month periods} = \frac{\textbf{End Index}}{\textbf{Start Index}}$$

2. Calculate the escalation rate by dividing the number found in Step 1 by 4:

Average Escalation Rate = (Escalation over (4) (12) month periods) / 4

3. Use the Average Escalation Rate found in Step 2 to determine EAP prices for years 6 - 10 of the contract as follows:
   - Year[1] 6 EAP Price = (Year 5 **Rate**) * (Average Escalation Rate)
   - Year 7 EAP Price = (Year 6 EAP Price) * (Average Escalation Rate)
   - Year 8 EAP Price = (Year 7 EAP Price) * (Average Escalation Rate)
   - Year 9 EAP Price = (Year 8 EAP Price) * (Average Escalation Rate)
   - Year 10 EAP Price = (Year 9 EAP Price) * (Average Escalation Rate)

The following procedure shall be used for Option Period 2:

4. Determine the escalation rate over four years by dividing the value of the Option Period 2 **End Index** by the value of the Option Period 2 **Start Index**:

$$\text{Escalation over (4) (12) month periods} = \frac{\textbf{End Index}}{\textbf{Start Index}}$$

5. Annualize the escalation rate by dividing the number found in Step 4 by 4.

Average Escalation Rate = (Escalation over (4) (12) month periods) / 4

[1] The term Year in this context is defined as the 12 consecutive months that are specified in the spreadsheet in J.15

6. Use the Annual Escalation Rate found in Step 5 to determine EAP prices for years 11 -15 of the contract as follows:
    - Year 11 EAP Price = (Year 10 **Rate**) * (Average Escalation Rate)
    - Year 12 EAP Price = (Year 11 EAP Price) * (Average Escalation Rate)
    - Year 13 EAP Price = (Year 12 EAP Price) * (Average Escalation Rate)
    - Year 14 EAP Price = (Year 13 EAP Price) * (Average Escalation Rate)
    - Year 15 EAP Price = (Year 14 EAP Price) * (Average Escalation Rate)

f) If the market indicator is discontinued or deemed no longer available or reliable by the government, the government and the contractor will mutually agree to a substitute. The contract modification reflecting the price adjustment will be effective upon approval by the CO. The adjusted prices shall apply to orders issued to the contractor on or after the effective date of the contract modification.

g) In any contract period during which price increases will be considered, the aggregate of the increases during any 5-year period shall not exceed ten percent (10%) of the contract unit price in effect at the end of the preceding 5-year period. The government reserves the right to raise the ceiling when market conditions during the contract period support such a change.

h) The government reserves the right to exercise one of the following options:

1. Accept the contractor's price adjustments as requested when all conditions of this clause are satisfied;
2. Negotiate more favorable prices when the total adjustment requested is not supported; or,
3. Decline the price adjustment when the request is not supported.

H.20 Hosting and Management of Government-Furnished Property (GFP)

Prior to the delivery of GFP, the contractor shall inform the government of all usual and customary or otherwise known, fees, charges, duties, taxes, surcharges, customs, laws, certifications, declarations or any other special requirements that are necessary to transport, or obtain approvals and authority to deliver and operate GFP at the contractor’s facility, or ship GFP from the contractor’s facility.

At the contractor’s facility, the contractor shall be responsible for the following, as required:

a) Maintaining, at the contractor’s expense, adequate public liability and property damage insurance, during the continuance of this contract, insuring the contractor against all claims for injury or damage.

b) Assuming responsibility for all damage or injury to persons or property occasioned through the use, maintenance, management, and operation of the contractor's facilities, GFP, or other equipment by, or by the action of, the contractor or contractor's employees and agents. The government shall in no event be liable or responsible for damage or injury to any person or property occasioned through the use, maintenance, management, or operation of any facility, GFP, or other equipment by, or by the action of, the contractor or the contractor's employees and agents in performing under this contract, and the government shall be indemnified against claims for damage or injury in such cases.

c) Completing any necessary pre-delivery preparations for the delivery site, site security, or storage facilities to temporarily or permanently accommodate the GFP in a safe and secure manner.

d) Accepting, inspecting and verifying GFP inventory, including the processing and distribution of manifest records and receipts; uncrating, unpacking, and reporting and filing claims with transporters for damaged or missing GFP.

e) Relocating GFP from initial receiving points or temporary storage facilities to the final contractor facility and installation site.

f) Preparing the final installation site including the provisioning of necessary physical space, environmental systems, and network connectivity, including but not limited to: internetworking connections, fire suppression, HVAC, power, lighting, water, sewer, telephone and communications, physical security systems, network security systems, disaster resistance and recovery systems, cages, racks, and UPS, emergency power systems, all on a 24x7 basis, unless otherwise mutually agreed upon and specified.

g) GFP setup, including assembling, loading, configuring, testing, filing warranty and guarantee documents, and certifications. Determinations of inter-compatibility and inter-operability shall be conducted by the contractor as soon as practical after delivery and setup.

h) Providing contractor personnel with all required national citizenship, security clearances, training, and technical certifications to receive, use, maintain, manage, operate, package, transport, or ship sensitive and secure GFP.

i) Providing training as requested by the government, on a per/seat and location basis, for government personnel as appropriate for the installation, configuration, operation, maintenance, and management of GFP.

j) Providing all usual and customary testing equipment (i.e., voltage, current and continuity testers, wireless LAN test tools, inline network testers, cable and wire

testers, optical echo testers, etc.) as required for quality assurance purposes and diagnostic testing of GFP.

k) Certifying GFP is in working order prior to crating and packing for return shipment, safe-guarding and escorting GFP to the transport carrier's departure point, and signing over GFP to the government provided or approved transport carrier. The cost of crating and packing, and any interim transportation to the point-of-transfer to the government provided or approved transport carrier shall be provided by the contractor free of expense to the government.

GFP shall be crated, packaged and delivered to the contractor's facility at the government's expense, unless otherwise agreed upon and approved by the government and the contractor.

At the government's option, the contractor shall provide or subcontract for GFP maintenance, if available.

Authorized government personnel shall have access to GFP at specified times, in specified locations, as mutually agreed upon between the government and the contractor. Government personnel will conform to the contractor's Acceptable Use Policy (AUP) in effect at the specified contractor facility, except where the AUP conflicts with agency regulations, the provisions of the contract, or other government executive orders, regulations or laws.

H.21 Notice to Proceed

The contractor will receive a written Notice to Proceed (NTP) from the CO after contract award. The NTP authorizes the contractor to:

- Respond to agency requirements issued as part of fair opportunity.
- Submit deliverables as required by the contract.
- Submit and execute modifications to the contract.
- Begin other actions specifically authorized in the contract.
- Prepare for BSS and security testing.

The NTP does not authorize the contractor to accept and process task orders or service orders, provision or deliver services, or bill for services. The contractor may only accept and process task orders or service orders, provision or deliver services and bill for services after it receives written notification 1) from the CO that it has passed BSS testing and 2) from GSA that it has successfully completed security testing in accordance with G.5.6.

The NTP shall also include contact information for the GSA CO, PM, COR(s), TSMs, and contacts with the GSA PMO.

H.22 Meetings/conferences

Meetings and/or post-award/pre-performance conferences and/or meetings during contract performance may be necessary to resolve problems and to facilitate understanding of the requirements of the contract. Participants at these meetings/conferences shall be members of the contractor's staff and representatives of the government. These meetings/conferences shall be scheduled with the agreement of and arrangements made between the OCO or the OCO's representative and the contractor. All contractor costs associated with the attendance at these meetings shall be incidental to the contract and not be separately billed.

H.23 Fees and Surcharges

The government generally will pay all allowable government-imposed and regulatory-based fees and surcharges, which shall only be assessed against jurisdictionally interstate traffic, applicable to telecommunications services delivered under this contract with the following exceptions:

- Fees and surcharges from which the Federal Government is expressly exempt under the authorizing state statute or local ordinance.
- Any fee or surcharge whose legal incidence is on the Federal Government.
- Any fee or surcharge that includes or allows for the recovery of vendor's administrative costs regardless if the vendor recovers those costs

Fees and surcharges shall not be included in the CLIN price, and shall be billed separately from the CLIN prices (see Agency Request for Fully Loaded CLIN Prices for opposite treatment).

Special attention must be paid to the treatment of the Associated Government Fee (AGF), which will be included in the prices of services as explained in Section J.2.10. The contractor shall not include fees and surcharges in its AGF calculation when fees and surcharges are billed separately from the CLIN price (see Agency Request for Fully Loaded CLIN Prices for opposite treatment). For example, the contractor shall not include the AGF when calculating the EIS revenues to which a fee or surcharge applies. The exclusion of the AGF is for the purposes of fee and surcharge calculations only; for all other billing purposes the AGF shall be handled in accordance with the billing processes.

All fees and surcharges shall be included in the tax file referenced in H.14. The fees and surcharges in the file may be invoiced by a contractor in accordance with the following:

- The fee or surcharge is applicable to the service in question
- The fee or surcharge is invoiced at the proper rate
- The invoice includes the citation from the file

If a contractor needs to invoice a fee or surcharge that is not in the file, the contractor must provide the following 30 days prior to including the fee or surcharge in question on an invoice:

- The name of each fee or surcharge
- The jurisdiction by name
- The statutory source (include web reference if possible) for the fee or surcharge
- The applicable fee or surcharge rate(s)

The CO will notify the contractor within 30 days after receipt of the information above as to whether or not the fee or surcharge is allowable under the terms and conditions of the contract. If the fee or surcharge is deemed allowable, it will be added to the file within 15 days.

The contractor and the government shall follow the same process outlined above when notifying the CO of “after-imposed taxes” as defined in FAR Clause 52.229-4.

The contractor shall provide to the government, on a semi-annual basis, an itemized list of fees or surcharges that are included in its monthly invoices, including the name of each fee or surcharge, jurisdiction by name, reference to the statutory source for the fee or surcharge, and applicable fee or surcharge rates. See Section F for the specific deliverable.

Agency Request for Fully Loaded CLIN Prices

A direct billed agency may elect, at its discretion, to request that all allowable fees and surcharges be included in the CLIN prices proposed in response to an agency task order solicitation. For any task order requiring that all allowable fees and surcharges be included in the CLIN prices, the ordering agency will be responsible for ensuring that only applicable and allowable fees and surcharges have been assessed and included in the CLIN prices. The AGF shall be assessed on the fully loaded CLIN prices under this option.

H.24 U.S. Citizenship Requirements

The contractor is hereby placed on notice that work on some orders, especially those requiring site visits to some U.S. Government locations or work on some Government Furnished Property, may require contractor personnel performing the work to have U.S. citizenship and to be able to provide proof of that citizenship. This shall be provided at no additional cost to the government.

H.25 Service Trials

A service trial is defined as the use of proposed future enhancements by an agency that takes place for an agreed upon period of time, at agreed upon location(s). The contractor shall provide written notification to the GSA CO and the OCO prior to initiation of any trial program with the agency. This notification shall include the start date and duration and a copy of the estimate for collateral costs. The contractor may invoice the government for collateral costs. These collateral costs shall be limited to the components of the service that are already in the contract and shall be at contract prices. The contractor shall not invoice the government for any items not already in the contract.

The contractor shall provide the OCO with contract prices and the corresponding section(s) of the contract that the trial proposes to enhance. The OCO will respond with approval or rejection. The contractor will not be reimbursed for trial costs exceeding the collateral cost estimate unless approval for such costs has been made by the OCO in writing prior to the start of the service trial.

The requiring agency, independent of GSA, will be responsible for the establishment of performance standards and making a determination of acceptability for the service. The agency shall use these standards to evaluate the service.

Service trials are not an exception to the fair opportunity process in Section G.3.1.

The contractor shall report monthly and upon the completion of each trial to the OCO in writing using the format and data in Table H.25-1 below:

a) Number of trials.

b) Description of the trials.

c) Participants.

d) Location(s).

e) Results to date.

f) Estimated completion dates.

g) Estimated costs (if applicable).

H.25.1 Service Trial Status Report Table

Service Trial Status Report					
Number of Trials					
Trial Description	**Participants**	**Location(s)**	**Results to Date**	**Estimated Completion Date**	**Estimated Cost (if applicable)**

H.26 Release of EIS Current Year Unit CLIN Prices

The government intends to release the current contract-year Unit CLIN prices after contract award. Each period will be updated with current contract price modifications. The contractor names associated with the prices will be included with the pricing information.

H.27 Acceptable Use Policy

The following Acceptable Use Policy (AUP) applies:

This Acceptable Use Policy (AUP) shall prevail over the terms of any other AUP used by the contractor or any of its subcontractors, suppliers or teaming partners. Any inconsistency between this AUP and any government requirements in the contract shall be resolved by giving precedence to the government requirements in the contract. This AUP may only be changed through contract modification.

Legitimate Government Use

This AUP does not limit the ability of customers to carry out legal operations pursuant to their regulatory, law-enforcement, or national defense responsibilities.

Prohibited Actions

Services provided under this contract may only be used for lawful purposes. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. Interference with the use of the contractor's network or the Internet, or use of services provided under the contract that results in the publication of threatening or offensive material, the distribution of forged or unsolicited e-mails ("spam") or other E-mail/Usenet abuse, or use that presents security or privacy risks for other than valid government requirements is prohibited.

Unlawful Activities

Customers may not use the services provided under the contract in criminal or civil violation of any applicable local, state, or federal law, treaty, court order, ordinance, regulation or administrative rule.

Intellectual Property

Pursuant to 28 U.S.C. 1498, the exclusive action which may be brought for government use of the contractor's service to transmit, re-transmit, or store any content or to engage in any activity that infringes the intellectual property rights of any individual, group or entity is an action by the intellectual property owner against the United States in the United States Court of Federal Claims.

Threatening or Offensive Material or Content

Except as required in connection with the execution of lawful, duly authorized government operations, customers may not use the services provided under the contract to host, post, transmit, or re-transmit any content or material that is threatening, harassing, obscene, indecent, pornographic, hateful, malicious, racist, defamatory, libelous, treasonous, excessively violent or promotes the use of violence, or provides instruction, information or assistance in causing or carrying out violence against any government, organization, group or individual, or provides guidance, information or assistance with respect to causing damage or security breaches to the contractor's network or to the network of any other service provider under this contract.

E-mail Abuse

Except as required in connection with the execution of lawful, duly authorized government operations, customers may not use the services provided under this contract to send or facilitate the sending of forged or unsolicited e-mail messages, including the sending of "junk e-mail" or other advertising material to individuals who did not specifically request such material ("e-mail spam").

Security Violations

Except as required in connection with the execution of lawful, duly authorized government operations, customers may not use the services provided under the contract to interfere with, to gain unauthorized access to or to otherwise violate the security of the contractor's or another's server, network, personal computer, network access or control devices, software or data, or other system, or to attempt to do any of the foregoing.

Customer Responsibilities

Customers remain solely and fully responsible for their content and for their use of the services provided under the contract only for legitimate government requirements and operations.

Suspension of Service

The contractor shall provide written notice to the OCO with a detailed explanation of an AUP violation so that such violation may be corrected without impact on service. In the event the agency is not successful, the contractor may, only to the extent necessary to prevent the continued violation of the AUP, suspend the service. Said suspension shall be effective no earlier than five (5) business days after the government has acknowledged receipt of the written notice of an AUP violation. The government is deemed to have received notice twenty-four (24) hours after written notice has been sent via confirmed e-mail.

Notwithstanding the foregoing, the contractor may, 24 hours after the OCO has acknowledged receipt of the contractor's written notice and detailed explanation, suspend service only to the extent necessary to prevent a violation of this AUP from causing imminent (1) exposure of the contractor or underlying service providers to criminal sanctions or prosecution, (2) significant irreparable harm to or significant interference with the integrity or normal operations or security of the contractor's network or networks with which the contractor is interconnected or significant interference with another customer's use of the contractor services or the Internet; (3) significant irreparable harm to the contractor, underlying service providers, the contractor's customers, or their respective employees. The government is deemed to have received notice twenty-four (24) hours after written notice has been sent via confirmed fax or e-mail.

The contractor may act immediately and without prior notice to suspend service only to the extent necessary to respond to a federal or state government order or mandate that certain conduct must be stopped. In such instance, the contractor shall provide written notice and detailed explanation to the GSA CO, and the impacted agency OCO within 30 minutes of its receipt of the court or other government order mandating service suspension.

Under no circumstances may the contractor suspend service without notice.

Any suspension shall be only for the time necessary for steps to be taken that will reasonably prevent the violation from continuing or reoccurring.

Under no circumstances may the contractor unilaterally terminate service.

H.28 Reserved

H.29 Open Season On-Ramping New Contractors

Consistent with FAR 16.504(c)(1)(ii)(A), the GSA CO has determined that it is in the government's best interest that at all times during the term of the contract, there remain an adequate number of EIS contractors eligible to compete for orders. Over time, the total number of EIS contractors may fluctuate due to various reasons including industry consolidation, industry technological adoption, general economic conditions, or other reasons. Recognizing this, GSA intends to review the total number of EIS contractors during the period of performance and determine whether it would be in the government's best interest to initiate an on-ramp process to award additional contracts in order to maintain competition.

H.29.1 On-Ramp Procedures

If the CO determines that it would be in the government's best interest to open the EIS RFP to add new contractors to this contract, the CO may do so at any time during the period of performance provided that:

a) The solicitation is issued under then-applicable federal procurement law.

b) Any contractor that meets the eligibility requirements set forth in the new solicitation submits an acceptable proposal in response to the solicitation.

c) The award decision under any solicitation is based upon substantially the same evaluation factors/sub-factors as the original solicitation.

d) The terms and conditions of any resulting awards from a new solicitation are materially identical to the existing version of the EIS RFP.

e) The term for any such new awards from a solicitation is co-terminus with the existing term for all other EIS contracts, including the option period (if applicable).

f) The award of any new contract(s) does not increase the overall ceiling of the acquisition.

g) The MRG shall be negotiated if and when the procedures in this clause are invoked.

H.30 Expansion of Core Based Statistical Areas

The contractor may, by way of bilateral modification, expand its service offerings and coverage beyond those Core Based Statistical Areas (CBSAs) awarded initially in the contract. The contractor may submit a proposal to this effect to the GSA CO during the contract life after receiving the Notice to Proceed. Submissions shall include:

1. All applicable mandatory services for each CBSA.

2. All applicable mandatory price tables and price elements, using the GSA-provided price proposal submission software. Note that, as with the original solicitation, the contractor may propose additional mandatory services coverage for CBSAs where no services are found in the traffic model.
3. Updates to contractor's proposal sections as appropriate to meet the minimum mandatory requirements set forth in the original EIS solicitation, including any subsequent amendments.

GSA reserves the right to update the traffic model any time during the contract life. The GSA CO must find all pricing to be fair and reasonable. If the proposal is not deemed so, the CO may reject the proposal for additional CBSA(s) in whole or in part, and award none, some, or all proposed additional CBSAs to the contractor. CBSAs are defined in OMB Bulletin No. 13-01, dated February 28, 2013.

H.31 Use of Transaction Data

Contractor(s) must ensure transaction data generated in the performance of the contract will not be used for data mining or analysis except for security without the express written consent of the GSA CO or OCO.

H.32 Payments and Incorrectly Invoiced Items

Notwithstanding the Payment clauses (52.232-1, 52.232-5, 52.232-6, 52.232-7, 52.232-25) , the government reserves the right to either reject the invoice in accordance with those clauses or withhold payment for any individual charge on an invoice that does not match the price on the contract and/or task order.

H.33 E-Discovery for Cloud-Based Services

The contractor shall provide electronically stored information (ESI) requests/searches within in 15 days of a written request by the GSA CO and/or OCO. Upon the written notice, the contractor shall follow the following preservation actions with no additional cost to the government:

Definitions

Preservation should be interpreted broadly to accomplish the goal of identifying all potentially relevant documents, maintaining the integrity of the documents as they currently exist and ensuring that they are not altered, deleted, destroyed or otherwise modified. If the contractor has any doubt as to whether a document or category of documents is covered by this clause, it should err on the side of preservation. The contractor's obligation to preserve extends to all potentially relevant documents in its possession, custody or control. Examples of documents that are not in the contractor's possession or custody, but remain subject to its control, include documents in the

possession or custody of contractor employees, or documents in the possession or custody of third parties such as subcontractors.

This clause requires only that the contractor preserve potentially relevant documents. The contractor should NOT copy, move, forward or otherwise collect potentially relevant documents unless directed to do so by the GSA CO and/or agency OCOs. This is especially critical for ESI, as there is electronic information ("metadata") that does not appear on the printed version of an electronic document, but provides critical information about the data and must be preserved, along with any directory and/or folder information about where the data is stored.

What to Preserve

The contractor must not alter, delete, destroy or otherwise modify potentially relevant documents. Please note that the contractor must preserve all non-identical copies of potentially relevant documents, so if one copy contains handwritten notes and the other does not, both should be preserved. Similarly, drafts of potentially relevant documents, to the extent they exist, should be preserved. Unless otherwise stated, the relevant time period begins on the date of contract award, and continues into the future.

Retention period for all preservation of e-Discovery data is consistent with GSAR clause 552.215-70.

H.34 Tariff Filing Requirements

a) The contractor shall file all domestic and/or non-domestic tariff or any other regulatory filings that are required by law or regulation and that are necessary for contract performance. The contractor shall provide the GSA CO copies of all such filings on the same day they are filed. The contractor shall certify that all terms, conditions, and prices in the filing are as stated in the contract, and that the filing contains nothing inconsistent with the contract. Refer to Section F for deliverable requirements.

b) The contractor shall file the initial tariff filing(s) required to implement the contract within sixty (60) days after the date of Notice to Proceed. If such filing(s) is not permitted to become effective by a governmental regulatory body or bodies within one-hundred and five (105) days after the date of Notice to Proceed, the government shall have the right, partially or entirely, to terminate the contract without liability.

c) After contract award, except for the initial filing mentioned in (b) above, the contractor shall provide to the GSA CO advance copies of all revisions to existing tariffs, new tariffs, or other regulatory filings that specifically pertain to the contract or that may materially affect the government's rights under the contract. These shall be

provided to the CO at least ten (10) days in advance of the intended filing date. The contractor shall make no revisions to its tariffs or other regulatory filings that materially and adversely affect the government's rights under the contract (including the contract as modified), without obtaining the government's prior written consent.

d) If any ruling, order, or determination of the governmental regulatory body or a court of competent jurisdiction shall materially and adversely affect the contractor's ability to offer services under the terms and conditions of this contract, the contractor shall immediately develop a proposal that provides comparable service to the government at rates equal to or less than those set forth in the contract, and under terms and conditions identical to those set forth in the contract, to the extent permissible under applicable legal and regulatory requirements.

H.35 Security Clearance Requirements

To ensure the capability to respond to Top Secret requirements, the contract includes a DD Form 254 (Contract Security Classification Specification) in Section J.14 A Top Secret Facility Clearance is not required to be eligible for receiving an EIS contract award; however, it may be required to meet agency specific task order requirements. The DD Form 254 will reflect a Top Secret Facility Clearance with no safeguarding, special access or communications security (COMSEC) requirements. The contractor may request this clearance from GSA after issuance of NTP. However, task orders may require and identify safeguarding, special access and security requirements. Additional requirements may also be identified on the agency-specific DD Form 254. When classified work is required on a task order, the DD Form 254 or agency equivalent will be issued by the OCO.

The contractor is responsible for providing personnel with appropriate security clearances to ensure compliance with government security regulations, as specified on task orders. The contractor shall fully cooperate on all security checks and investigations by furnishing requested information to verify the contractor employee's trustworthiness and suitability for the position.

H.36 Subcontracting Plan and Additional Monitoring

a) Definitions. As used in this clause:

1. "Subcontract" means any contract as defined in Subpart 2.1 entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract. It includes but is not limited to purchase orders, and changes and modifications to purchase orders.
2. "Subcontractor" means any supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor.

3. Costs associated with acquiring service(s) from Local Exchange Carriers (LECs) under this contract are excluded from the definition of subcontracting for the purposes of eSRS reporting.

b) The contractor is required to adhere to the subcontracting plan incorporated into this contract. As such, the contractor shall report subcontract information.

c) The government intends to monitor the contractor's adherence to the subcontracting plan and continually work to ensure the maximum practicable participation of these business concerns. The contractor's performance will be reported in the Past Performance Information Retrieval System (PPIRS). In addition to the requirement to file Individual Subcontracting Reports (ISR) and Summary Subcontracting Reports (SSR), as required in FAR 52.219-9, and submitted in Electronic Subcontracting Reporting System (eSRS), the contractor shall provide to the GSA CO subcontracting information cited below. In support of the government's monitoring effort, the contractor shall, on a semiannual basis:

1. Provide a concise written summary of activity in the contractor's subcontracting outreach program (as described in the contractor's subcontracting plan).
2. Provide subcontracting plan backup data (in MS Excel) consisting of a spreadsheet showing, in chronological order of subcontract award, the dollar-value of each subcontract, type of subcontract and the name and size of the business concern to which the subcontract was awarded.

H.37 Supply Chain Risk Management (SCRM)

a) Definitions. As used in this clause:

"Information technology" (see 40 U.S.C 11101(6)) means, in lieu of the definition at FAR 2.1, any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

1. For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires:
   i. Its use; or
   ii. To a significant extent, its use in the performance of a service or the furnishing of a product.
2. The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

3. The term “information technology” does not include any equipment acquired by a contractor incidental to a contract.

“Supply chain risk,” means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to survey, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

b) The contractor shall maintain controls in the provision of supplies and services to the government to minimize supply chain risk.

c) In order to manage supply chain risk, the government may use the authorities provided by section 806 of Pub. L. 111-383. In exercising these authorities, the government may consider information, public and non-public, including all-source intelligence, relating to a contractor’s supply chain.

d) If the government exercises the authority provided in section 806 of Pub. L. 111-383 to limit disclosure of information, no action undertaken by the government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

e) The contractor shall include the substance of this clause, including this paragraph e), in all subcontracts involving the development or delivery of any information technology, whether acquired as a service or as a supply.

H.38 Force Majeure Notification

a) The contractor shall not be liable for any excess costs if the failure to perform the contract arises from causes beyond the control and without the fault or negligence of the contractor. Examples of such causes include (1) acts of God or of the public enemy, (2) acts of the government in either its sovereign or contractual capacity, (3) fires, (4) floods, (5) epidemics, (6) quarantine restrictions, (7) freight embargoes, and (8) unusually severe weather. In each instance, the failure to perform must be beyond the control and without the fault or negligence of the contractor.

b) If the failure to perform is caused by the default of a subcontractor at any tier, and if the cause of the default is beyond the control of both the contractor and subcontractor, and without the fault or negligence of either, the contractor shall not be liable for any excess costs for failure to perform, unless the subcontracted supplies or services were obtainable from other sources in sufficient time for the contractor to meet the required delivery schedule.

c) The contractor shall provide written notification to the OCO if the contractor is citing one of the causes in paragraph a) above as its reason for failure to perform. The notification must be submitted within 10 days of the cause the contractor is citing as the reason for non-performance. The OCO shall ascertain the facts and extent of the failure. If the OCO determines that any failure to perform results from one or more of the causes above, the delivery schedule shall be revised, subject to the rights of the government under the termination clause of this contract.

Enterprise Infrastructure Solutions (EIS)

~~Request for Proposals~~Contract

Section I

Contract Clauses

Issued by:

General Services Administration

Office of ~~Integrated~~Information Technology ~~Services~~Category

[redacted]

~~JULY 2017~~January 2019

Table of Contents

I.1 General

Orders under the contract may include additional clauses to those enumerated in this contract, such as: (1) optional FAR clauses; (2) agency supplemental clauses; (3) alternate FAR clauses; and (4) order-specific clauses. Such additional clauses are not limited to those associated only with Section I of the Uniform Contract Format in FAR 52.3.

The clauses relating to the Wage Rate Requirements (Construction), formerly known as the Davis-Bacon Act (52.222-13 and 52.222-30), shall be included in a task order by the ordering contracting officer (OCO) if it is deemed applicable to the order.

The clauses in Section I.2 apply at the at the contract and order levels, as applicable, depending upon the contract type of the order, or as specifically referenced in the applicable order.

I.2 FAR 52.252-2 Clauses Incorporated By Reference (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the contracting officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses:

FEDERAL ACQUISITION REGULATION:

https://acquisition.gov/far/index.html

GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL:

https://acquisition.gov/gsam/gsam.html

I.2.1 FAR 52.252-2 Clauses Table

CLAUSE NO.	TITLE	DATE	FP	T&M
52.202-1	Definitions	NOV 2013	X	X
52.203-3	Gratuities	APR 1984	X	X
52.203-5	Covenant Against Contingent Fees	MAY 2014	X	X
52.203-6	Restrictions on Subcontractor Sales to the Government	SEP 2006	X	
52.203-7	Anti-Kickback Procedures	MAY 2014	X	X

CLAUSE NO.	TITLE	DATE	FP	T&M
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	MAY 2014	X	X
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	MAY 2014	X	X
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	OCT 2010	X	X
52.203-13	Contractor Code of Business Ethics and Conduct	OCT 2015	X	X
52.203-14	Display of Hotline Poster(s)	OCT 2015	X	X
52.203-16	Preventing Personal Conflicts of Interest	DEC 2011	X	X
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	APR 2014	X	X
52.204-2	Security Requirements	AUG 1996	X	X
52.204-4	Printed or Copied Double-Sided on Recycled Paper	MAY 2011	X	X
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011	X	X
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	OCT 2015	X	X
52.201-12	Data Universal Numbering System Number Maintenance	DEC 2012	X	X
52.204-13	System for Award Management Maintenance.	OCT 2016	X	X
52.204-15	Service Contract Reporting Requirements for Indefinite-Delivery Contracts	JAN 2014	X	X
52.204-18	Commercial and Government Entity Code Maintenance	JUL 2015	X	X
52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018).	JUL 2018	X	X
52.207-3	Right of first refusal of employment	MAY 2006	X	X
52.207-5	Option to purchase equipment	FEB 1995	X	X
52.209-6	Protecting the government's interest when subcontracting with contractors debarred, suspended, or proposed for debarment	AUG 2013	X	X
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	JUL 2013	X	X

CLAUSE NO.	TITLE	DATE	FP	T&M
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	DEC 2014	X	X
52.210-1	Market Research	APR 2011	X	X
52.211-5	Materials Requirements	AUG 2000	X	
52.211-15	Defense Priority and Allocation Requirements	APR 2008	X	X
52.215-2	Audit and Records – Negotiation	OCT 2010	X	X
52.215-2	Alternate II	APR 1998	X	X
52.215-2	Alternate III	JUN 1999	X	X
52.215-8	Order of Precedence – Uniform Contract Format	OCT 1997	X	X
52.215-10	Price Reduction for Defective Cost or Pricing Data	AUG 2011	X	X
52.215-11	Price Reduction for Defective Cost or Pricing Data – Modifications	AUG 2011	X	X
52.215-12	Subcontractor Cost or Pricing Data	OCT 2010	X	X
52.215-13	Subcontractor Cost or Pricing Data – Modifications	OCT 2010	X	X
52.215-14	Integrity of Unit Prices	OCT 2010	X	X
52.215-16	Facilities Capital Cost of Money	JUN 2003	X	X
52.215-19	Notification of Ownership Changes	OCT 1997	X	X
52.216-4	Economic Price Adjustment – Labor and Material	JAN 1997	X	X
52.217-6	Option for Increased Quantity	MAR 1989	X	
52.217-7	Option for Increased Quantity – Separately Priced Line Item	MAR 1989	X	
52.219-4	Notice of Price Evaluation Preference for HUBZone Small Business Concerns	OCT 2014	X	X
52.219-8	Utilization of Small Business Concerns	OCT 2014	X	X
52.219-9	Small Business Subcontracting Plan	JAN 2017	X	X
52.219-9	Alternate II	JAN 2017	X	X
52.219-16	Liquidated Damages – Subcontracting Plan	JAN 1999	X	X

CLAUSE NO.	TITLE	DATE	FP	T&M
52.222-1	Notice to the Government of Labor Disputes	FEB 1997	X	X
52.222-2*	Payment for Overtime Premiums	JUL 1990	X	X
52.222-3	Convict Labor	JUN 2003	X	X
52.222-4	Contract Work Hours and Safety Standards – Overtime Compensation	MAY 2014	X	X
52.222-6	Construction Wage Rate Requirements.	MAY 2014	X	X
52.222-7	Withholding of Funds	MAY 2014	X	X
52.222-8	Payrolls and Basic Records	MAY 2014	X	X
52.222-9	Apprentices and Trainees	JUL 2005	X	X
52.222-10	Compliance with Copeland Act Requirements	FEB 1988	X	X
52.222-11	Subcontracts (Labor Standards)	MAY 2014	X	X
52.222-12	Contract Termination – Debarment	MAY 2014	X	X
52.222-13*	Compliance with Construction Wage Rate Requirements and Related Regulations	MAY 2014	X	X
52.222-14	Disputes Concerning Labor Standards	FEB 1988	X	X
52.222-15	Certification of Eligibility	MAY 2014	X	X
52.222-17	Non-displacement of Qualified Workers	MAY 2014	X	X
52.222-19	Child Labor – Cooperation with Authorities and Remedies	FEB 2016	X	X
55.222-20	Contracts for Materials, Supplies, Articles, and Equipment Exceeding $15,000	MAY 2014	X	
52.222-21	Prohibition of Segregated Facilities	APR 2015	X	X
52.222-26	Equal Opportunity	APR 2015	X	X
52.222-27	Affirmative Action Compliance Requirements for Construction	APR 2015	X	X
52.222-29	Notification of Visa Denial	APR 2015	X	X
52.222-30*	Construction Wage Rate Requirements – Price Adjustment (None or Separately Specified Method)	MAY 2014	X	X

CLAUSE NO.	TITLE	DATE	FP	T&M
52.222-35	Equal Opportunity for Veterans	OCT 2015	X	X
52.222-36	Equal Opportunities for Workers with Disabilities	JUL 2014	X	X
52.222-36	Alternate I	JUL 2014	X	X
52.222-37	Employment Reports on Veterans	FEB 2016	X	X
52.222-40	Notification of Employee Rights Under the National Labor Relations Act	DEC 2010	X	X
52.222-41	Service Contract Labor Standards	MAY 2014	X	X
52.222-42	Statement of Equivalent Rates for Federal Hires	MAY 2014	X	X
52.222-43	Fair Labor Standards Act and Service Contract Labor Standards – Price Adjustment (Multiple Year and Option Contracts)	MAY 2014	X	X
52.222-50	Combating Trafficking in Persons	MAR 2015	X	X
52.222-50	Alternate I	MAY 2015	X	X
52.222-54	Employment Eligibility Verification	OCT 2015	X	X
52.222-55	Minimum Wages Under Executive Order 13658	DEC 2015	X	X
52.223-3*	Hazardous Material Identification and Material Safety Data	JAN 1997	X	X
52.223-3*	Alternate I	JUL 1995	X	X
52.223-2	Affirmative Procurement of Bio-based Products under Service and Construction Contracts	SEP 2013	X	
52.223-5	Pollution Prevention and Right-to-know Information	MAY 2011	X	X
52.223-5	Alternate I	MAY 2011	X	X
52.223-5	Alternate II	MAY 2011	X	X
52.223-6	Drug-free Workplace	MAY 2001	X	X
52.223-10	Waste Reduction Program	MAY 2011	X	X
52.223-12	Refrigeration Equipment and Air Conditioners	MAY 1995	X	X
52.223-13	Acquisition of EPEAT Registered Imaging Equipment	JUN 2014	X	X

CLAUSE NO.	TITLE	DATE	FP	T&M
52.223-13	Alternate I	JUN 2014	X	X
52.223-14	Acquisition of EPEAT Registered Televisions	JUN 2014	X	X
52.223-15	Energy Efficiency in Energy-Consuming Products	DEC 2007	X	X
52.223-16	Acquisition of EPEAT-Registered Personal Computer Products	OCT 2015	X	X
52.223-16	Alternate I	JUN 2014	X	X
52.223-17	Affirmative Procurement of EPA-designated Items in Service and Construction Contract	MAY 2008	X	X
52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving	AUG 2011	X	X
52.224-1	Privacy Act Notification	APR 1984	X	X
52.224-2	Privacy Act	APR 1984	X	X
52.225-1	Buy American Act – Supplies	MAY 2014	X	
52.225-3	Buy American Act – Free Trade Agreements – Israeli Trade Act	MAY 2014	X	
52.225-5	Trade Agreements	FEB 2016	X	
52.225-8	Duty-free Entry	OCT 2010	X	X
52.225-10	Notice of Buy American Requirement – Construction Materials	MAY 2014	X	
52.225-11	Buy American – Construction Materials under Trade Agreements	FEB 2016	X	
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008	X	
52.225-14	Inconsistency between English Version and Translation of Contract	FEB 2000	X	X
52.227-1	Authorization and Consent	DEC 2007	X	
52,227-2	Notice and Assistance Regarding Patent and Copyright Infringement	DEC 2007	X	X
52.227-3	Patent Indemnity	APR 1984	X	
52.227-3*	Alternate I	APR 1984	X	
52.227-3*	Alternate II	APR 1984	X	
52.227-5*	Waiver of Indemnity	APR 1984	X	

CLAUSE NO.	TITLE	DATE	FP	T&M
52.227-9	Refund of Royalties	APR 1984	X	
52.227-14	Rights in Data – General	MAY 2014	X	X
52.227-14	Alternate I	DEC 2007	X	X
52.227-14*	Alternate II	DEC 2007	X	X
52.227-19	Commercial Computer Software License	DEC 2007	X	
52.228-3	Workers' Compensation Insurance (Defense Base Act)	JUL 2014	X	X
52.228-4	Workers' Compensation and War-hazard Insurance Overseas	APR 1984	X	X
52.228-5	Insurance – Work on a Government Installation	JAN 1997	X	
52.228-7	Insurance – Liability to Third Persons	MAR 1996	X	X
52.229-2	North Carolina State and Local Sales and Use Tax	APR 1984	X	X
52.229-4	Federal, State, and Local Taxes (State and Local Adjustments	FEB 2013	X	X
52.229-6	Taxes – Foreign Fixed-Price Contracts	FEB 2013	X	X
52.229-10*	State of New Mexico Gross Receipts and Compensating Tax	APR 2003		X
52.232-1	Payments	APR 1984	X	
52.232-5	Payments under Fixed-Price Construction Contracts	MAY 2014	X	
52.232-6	Payment under Communication Service Contracts with Common Carriers	APR 1984	X	
52.232-7*	Payments under Time-and-materials and Labor-hour Contracts	AUG 2012		X
52.232-8	Discounts for Prompt Payment	FEB 2002	X	X
52.232-9	Limitation on withholding of payments	APR 1984	X	X
52.232-11	Extras	APR 1984	X	
52.232-18	Availability of Funds	APR 1984	X	X
52.232-23	Assignment of Claims	MAY 2014	X	X
52.232-23	Alternate I	APR 1984	X	X

CLAUSE NO.	TITLE	DATE	FP	T&M
52.232-25	Prompt Payment	JUL 2013	X	X
52.232-25	Alternate I	FEB 2002		X
52.232-33	Payment by Electronic Funds Transfer – System for Award Management	JUL 2013	X	X
52.232-34	Payment by Electronic Funds Transfer – Other than System for Award Management	JUL 2013	X	X
52.232-36	Payment by Third Party	MAY 2014	X	X
52.232-37	Multiple Payment Arrangements	MAY 1999	X	X
52.233-1	Disputes	MAY 2014	X	X
52.233-1	Alternate I	DEC 1991	X	X
52.233-3	Protest after Award	AUG 1996	X	X
52.233-3	Alternate I	JUN 1985	X	X
52.233-4	Applicable Law for Breach of Contract Claim	OCT 2004	X	X
52.236-2	Differing Site Conditions	APR 1984	X	X
52.236-3	Site Investigation and Conditions Affecting the Work	APR 1984	X	X
52.236-5	Material and Workmanship	APR 1984	X	X
52.236-6	Superintendence by the Contractor	APR 1984	X	X
52.236-7	Permits and Responsibilities	NOV 1991	X	X
52.236-8	Other Contracts	APR 1984	X	X
52.236-9	Protection of Existing Vegetation, Structures, Equipment, Utilities, and Improvements	APR 1984	X	X
52.236-10	Operations and Storage Areas	APR 1984	X	X
52.236-12	Cleaning up	APR 1984	X	X
52.236-13	Accident Prevention	NOV 1991	X	X
52.236-13	Alternate I	NOV 1991	X	X
52.237-2	Protection of Government Buildings, Equipment, and Vegetation	APR 1984	X	X

CLAUSE NO.	TITLE	DATE	FP	T&M
52.237-3	Continuity of Services	JAN 1991	X	
52.237-9	Waiver of Limitation on Severance Payments to Foreign Nationals	MAY 2014		X
52.237-10	Identification of Uncompensated Overtime	MAR 2015	X	X
52.239-1	Privacy or Security Safeguards	AUG 1996	X	X
52.242-13	Bankruptcy	JUL 1995	X	X
52.242-14	Suspension of Work	APR 1984	X	X
52,242-15	Stop-work Order	AUG 1989	X	X
52.243-1	Changes – Fixed-price	AUG 1987	X	
52.243-1	Alternate I	APR 1984	X	
52.243-1	Alternate II	APR 1984	X	
52.243-1	Alternate III	APR 1984	X	
52.243-3	Changes – Time-and-materials or Labor-hours	SEP 2000		X
52.243-4	Changes	JUN 2007	X	
52.243-5	Changes and Changed Conditions	APR 1984	X	
52.243-7	Notification of Changes	APR 1984	X	X
52.244-2*	Subcontracts	OCT 2010		X
52.244-2	Alternate I	JUN 2007		X
52.244-5	Competition in Subcontracting	DEC 1996	X	
52.244-6	Subcontracts for Commercial Items	FEB 2016	X	X
52.245-1	Government Property	APR 2012	X	X
52.245-1	Alternate I	APR 2012	X	X
52.245-1	Alternate II	APR 2012	X	X
52.245-2	Government Property Installation Operation Services	APR 2012	X	X
52.245-9	Use and Charges	APR 2012	X	X

CLAUSE NO.	TITLE	DATE	FP	T&M
52.246-17	Warranty of Supplies of a Noncomplex Nature	JUN 2003	X	X
52.246-20*	Warranty of Services	MAY 2001	X	
52.246-21	Warranty of Construction	MAR 1994	X	X
52.246-21	Alternate I	APR 1984	X	X
52.246-23	Limitation of Liability	FEB 1997	X	
52.246-24	Limitation of Liability – High Value Items	FEB 1997	X	X
52.246-24	Alternate I	APR 1984	X	X
52.246-25	Limitation of Liability – Services	FEB 1997	X	X
52.247-1*	Commercial Bill of Lading Notations	FEB 2006	X	X
52.248-1*	Value Engineering	OCT 2010	X	
52.248-1	Alternate I	APR 1984	X	X
52.248-1	Alternate II	FEB 2000	X	X
52.248-1	Alternate III	APR 1984	X	X
52.248-3	Value Engineering – Construction	OCT 2015	X	X
52.248-3	Alternate I	APR 1984	X	X
52.249-1	Termination for Convenience of the Government (Fixed-Price) (Short Form)	APR 1984	X	
52.249-1	Alternate I	APR 1984	X	
52.249-2	Termination for Convenience of the Government (Fixed-Price)	APR 2012	X	
52.249-2	Alternate I	SEP 1996	X	
52.249-2	Alternate II	SEP 1996	X	
52.249-2	Alternate III	SEP 1996	X	
52.249-3	Termination for Convenience of the Government (Dismantling, Demolition, or Removal of Improvements)	APR 2012	X	X
52.249-3	Alternate I	SEP 1996	X	X

CLAUSE NO.	TITLE	DATE	FP	T&M
52.249-4	Termination for Convenience of the Government (Services) (Short Form)	APR 1984	X	
52.249-8	Default (Fixed-price Supply and Service)	APR 1984	X	
52.249-14	Excusable Delays	APR 1984		X
52.251-1	Government Supply Sources	APR 2012	X	X
52.253-1	Computer Generated Forms	JAN 1991	X	X

(Note: Clause numbers followed by an asterisk (*) require fill-ins by the OCO if determined applicable and incorporated into the Order.)

(End of Clause)

I.3 General Services Administration Acquisition Manual (GSAM), Incorporated by Reference

I.3.1 GSAM Clauses Table

CLAUSE #	CLAUSE TITLE	DATE
552.203-71	Restriction on Advertising	SEP 1999
552.204-9	Personal Identity Verification Requirements	OCT 2012
552.215-70	Examination of Records by GSA	FEB 1996
552.216-74	Task Order and Delivery Order Ombudsman	AUG 2010
552.217-70	Evaluation of Options	AUG 1990
552.219-75	GSA Mentor/Protégé Program	SEP 2009
552.228-5	Government as Additional Insured	MAY 2009
552.229-71	Federal Excise Tax – DC Government	SEP 1999

I.4 FAR 52.216-18 Ordering (OCT 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued in accordance with Section G.3.

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, this contract shall control.

(c) If mailed, a delivery order or task order is considered "issued" when the government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized by the Schedule.

I.5 FAR 52.216-19 Order Limitations (OCT 1995)

(a) *Minimum order*. When the government requires supplies or services covered by this contract in an amount of less than $1, the government is not obligated to purchase, nor is the contractor obligated to furnish, those supplies or services under the contract.

(b) *Maximum order*. The contractor is not obligated to honor:

(1) Any order for a single item in excess of $1 Billion;

(2) Any order for a combination of items in excess of $1 Billion;

(3) A series of orders within 10 days from the same ordering office that exceeds the limitation in subparagraph (1) or (2) above.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR), the government is not required to order a part of any one requirement from the contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within three (3) work days after issuance, with written notice stating the contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the government may acquire the supplies or services from another source.

(End of clause)

I.6 FAR 52.216-22 Indefinite Quantity (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified that is effective for the period stated in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The contractor shall furnish to the government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the “maximum.” The government shall order at least the quantity of supplies or services designated in the Schedule as the “minimum.”

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the contractor within the time specified in the order. The contract shall govern the contractor’s and government’s rights and obligations with respect to that order to the same extent as if the order were completed during the contract’s effective period; provided, that the contractor shall not be required to make any deliveries under this contract fifteen (15) years and nine (9) months after the effective date of the contract.

(End of clause)

I.7 FAR 52.217-8 Option to Extend Services (NOV 1999)

The government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The contracting officer may exercise the option by written notice to the contractor within 3 months of the end of the contract or order.

(End of clause)

I.8 FAR 52.217-9 Option to Extend the Term of the Contract (MAR 2000)

(a) The government may extend the term of this contract by written notice to the contractor within 30 days of the expiration of the contract; provided that the government gives the contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the government to an extension.

(b) If the government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 15 years and 9 months.

(End of clause)

I.9 FAR 52.252-6 Authorized Deviations in Clauses (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any GSAM (48 CFR Chapter 5) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

I.10 GSAM 552.232-39 Unenforceability of Unauthorized Obligations. (FAR Deviation)(JULY 2015)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any [commercial supplier agreement (as defined in 502.101)] that includes any [language, provision, or] clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(1) Any such [language, provision, or] clause is unenforceable against the Government.

(2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the [commercial supplier agreement. If the commercial supplier agreement] is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.

(3) Any such [language, provision, or] clause is deemed to be stricken from the [commercial supplier agreement].

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(End of Clause)

I.11 GSAM 552.232-78 Commercial Supplier Agreements – Unenforceable Clauses (JULY 2015)

(a) When any supply or service acquired under this contract is subject to a commercial supplier agreement, the following language shall be deemed incorporated into the commercial supplier agreement. As used herein, "this agreement" means the commercial supplier agreement:

(1) Notwithstanding any other provision of this agreement, when the end user is an agency or instrumentality of the U.S. Government, the following shall apply:

(i) Applicability. This agreement is part of a contract between the commercial supplier and the U.S. Government for the acquisition of the supply or service that necessitates a license (including all contracts, task orders, and delivery orders not using FAR Part 12).

(ii) End user. This agreement shall bind the ordering activity as end user but shall not operate to bind a Government employee or person acting on behalf of the Government in his or her personal capacity.

(iii) Law and disputes. This agreement is governed by Federal law.

(A) Any language purporting to subject the U.S. Government to the laws of a U.S. state, U.S. territory, district, or municipality, or foreign nation, except where Federal law expressly provides for the application of such laws, is hereby deleted.

(B) Any language requiring dispute resolution in a specific forum or venue that is different from that prescribed by applicable Federal law is hereby deleted.

(C) Any language prescribing a different time period for bringing an action than that prescribed by applicable Federal law in relation to a dispute is hereby deleted.

(iv) Continued performance. If the supplier or licensor believes the ordering activity to be in breach of the agreement, it shall pursue its rights under the Contract Disputes Act or other applicable Federal statute while continuing performance as set forth in 52.233-1 Disputes.

(v) Arbitration; equitable or injunctive relief. In the event of a claim or dispute arising under or relating to this agreement, (A) binding arbitration shall not be used unless specifically authorized by agency guidance, and (B) equitable or injunctive relief, including the award of attorney fees, costs or interest, may be awarded against the U.S. Government only when explicitly provided by statute (e.g., Prompt Payment Act or Equal Access to Justice Act). 7

(vi) Additional terms. (A) This commercial supplier agreement may unilaterally incorporate additional terms by reference. Terms may be included by reference using electronic means (e.g., via web links, click and accept, etc). Such terms shall be enforceable only to the extent that:

(1) When included by reference using electronic means, the terms are readily available at referenced locations; and

(2) Terms do not materially change government obligations; and

(3) Terms do not increase government prices; and

(4) Terms do not decrease overall level of service; and

(5) Terms do not limit any other Government right addressed elsewhere in this contract.

(B) The order of precedence clause of this contract notwithstanding, any software license terms unilaterally revised subsequent to award that is inconsistent with any material term or provision of this contract is not enforceable against the government.

(vii) No automatic renewals. If any license or service tied to periodic payment is provided under this agreement (e.g., annual software maintenance or annual lease term}, such license or service shall not renew automatically upon expiration of its current term without prior express Government approval.

(viii) Indemnification. Any clause of this agreement requiring the commercial supplier or licensor to defend or indemnify the end user is hereby amended to provide that the U.S. Department of Justice has the sole right to represent the United States in any such action, in accordance with 28 U.S.C. 516.

(ix) Audits. Any clause of this agreement permitting the commercial supplier or licensor to audit the end user's compliance with this agreement is hereby amended as follows:

(A) Discrepancies found in an audit may result in a charge by the commercial supplier or licensor to the ordering activity. Any resulting invoice must comply with the proper invoicing requirements specified in the underlying Government contract or order.

(B) This charge, if disputed by the ordering activity, will be resolved through the Disputes clause at 52.233-1 ; no payment obligation shall arise on the part of the ordering activity until the conclusion of the dispute process.

(C) Any audit requested by the contractor will be performed at the contractor's expense, without reimbursement by the Government.

(x) Taxes or surcharges. Any taxes or surcharges which the commercial supplier or licensor seeks to pass along to the Government as end user will be governed by the terms of the underlying Government contract or order and, in any event, must be

submitted to the Contracting Officer for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the Government contract.

(xi) Non-assignment. This agreement may not be assigned, nor may any rights or obligations thereunder be delegated, without the Government's prior approval, except as expressly permitted under the clause at 52.232-23, Assignment of Claims.

(xii) Confidential information. If this agreement includes a confidentiality clause, such clause is hereby amended to state that neither the agreement nor the Federal Supply Schedule price list shall be deemed "confidential information." Issues regarding release of "unit pricing" will be resolved consistent with the Freedom of Information Act. Notwithstanding anything in this agreement to the contrary, the Government may retain any confidential information as required by law, regulation or its internal document retention procedures for legal, regulatory or compliance purposes; provided, however, that all such retained confidential information will continue to be subject to the confidentiality obligations of this agreement.

If any provision of this agreement conflicts or is inconsistent with the preceding subparagraph (a)(1), the provisions of subparagraph (a)(1) shall prevail to the extent of such inconsistency.)

(End of Clause)

I.12 GSAM 552.239-71 Security Requirements for Unclassified Information Technology Resources (JAN 2012)

(a) *General.* The contractor shall be responsible for information technology (IT) security, based on General Services Administration (GSA) risk assessments, for all systems connected to a GSA network or operated by the contractor for GSA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the contractor has physical or electronic access to GSA's information that directly supports the mission of GSA, as indicated by GSA. The term information technology, as used in this clause, means any equipment, including telecommunications equipment that is used in the automatic acquisition, storage, manipulation, management, control, display, switching, interchange, transmission, or reception of data or information. This includes major applications as defined by OMB Circular A-130. Examples of tasks that require security provisions include:

(1) Hosting of GSA e-government sites or other IT operations;

(2) Acquisition, transmission, or analysis of data owned by GSA with significant replacement cost should the contractor's copy be corrupted;

(3) Access to GSA major applications at a level beyond that granted the general public; *e.g.*, bypassing a firewall; and

(4) Any new information technology systems acquired for operations within the GSA must comply with the requirements of HSPD-12 and OMB M-11-11. Usage of the credentials must be implemented in accordance with OMB policy and NIST guidelines (*e.g.*, NIST SP 800-116). The system must operate within the GSA's access management environment. Exceptions must be requested in writing and can only be granted by the GSA Senior Agency Information Security Officer.

(b) *IT Security Plan.* The contractor shall develop, provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The contractor's IT Security Plan shall comply with applicable Federal laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002, and the E-Government Act of 2002. The plan shall meet IT security requirements in accordance with Federal and GSA policies and procedures. GSA's Office of the Chief Information Officer issued "CIO IT Security Procedural Guide 09–48, Security Language for Information Technology Acquisitions Efforts," to provide IT security standards, policies and reporting requirements. This document is incorporated by reference in all solicitations and contracts or task orders where an information system is contractor owned and operated on behalf of the Federal Government. The guide can be accessed at http://www.gsa.gov/portal/category/25690. Specific security requirements not specified in "CIO IT Security Procedural Guide 09–48, Security Language for Information Technology Acquisitions Efforts" shall be provided by the requiring activity.

(c) *Submittal of IT Security Plan.* Within 30 calendar days after contract award, the contractor shall submit the IT Security Plan to the contracting officer and contracting officer's Representative (COR) for acceptance. This plan shall be consistent with and further detail the approach contained in the contractors proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as accepted by the contracting officer and COR, shall be incorporated into the contract as a compliance document. The contractor shall comply with the accepted plan.

(d) *Submittal of a Continuous Monitoring Plan.* The contractor must develop a continuous monitoring strategy that includes:

(1) A configuration management process for the information system and its constituent components;

(2) A determination of the security impact of changes to the information system and environment of operation;

(3) Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

(4) Reporting the security state of the information system to appropriate GSA officials; and

(5) All GSA general support systems and applications must implement continuous monitoring activities in accordance with this guide and NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

(e) *Security authorization.* Within six (6) months after contract award, the contractor shall submit written proof of IT security authorization for acceptance by the contracting officer. Such written proof may be furnished either by the contractor or by a third party. The security authorization must be in accordance with NIST Special Publication 800-37. This security authorization will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This security authorization, when accepted by the contracting officer, shall be incorporated into the contract as a compliance document, and shall include a final security plan, a risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan. The contractor shall comply with the accepted security authorization documentation.

(f) *Annual verification.* On an annual basis, the contractor shall submit verification to the contracting officer that the IT Security plan remains valid.

(g) *Warning notices.* The contractor shall ensure that the following banners are displayed on all GSA systems (both public and private) operated by the contractor prior to allowing anyone access to the system:

Government Warning

****WARNING****WARNING****WARNING****

Unauthorized access is a violation of U.S. law and General Services Administration policy, and may result in criminal or administrative penalties. Users shall not access other users or system files without proper authority. Absence of access controls IS NOT authorization for access! GSA information systems and related equipment are intended for communication, transmission, processing and storage of U.S. Government

information. These systems and equipment are subject to monitoring by law enforcement and authorized Department officials. Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed or stored in this system by law enforcement and authorized Department officials. Use of this system constitutes consent to such monitoring.

****WARNING**WARNING**WARNING****

(h) *Privacy Act notification.* The contractor shall ensure that the following banner is displayed on all GSA systems that contain Privacy Act information operated by the contractor prior to allowing anyone access to the system:

This system contains information protected under the provisions of the Privacy Act of 1974 (Pub. L. 93-579). Any privacy information displayed on the screen or printed shall be protected from unauthorized disclosure. Employees who violate privacy safeguards may be subject to disciplinary actions, a fine of up to $5,000, or both.

(i) *Privileged or limited privileges access.* Contractor personnel requiring privileged access or limited privileges access to systems operated by the contractor for GSA or interconnected to a GSA network shall adhere to the specific contract security requirements contained within this contract and/or the Contract Security Classification Specification (DD Form 254).

(j) *Training.* The contractor shall ensure that its employees performing under this contract receive annual IT security training in accordance with OMB Circular A-130, FISMA, and NIST requirements, as they may be amended from time to time during the term of this contract, with a specific emphasis on the rules of behavior.

(k) *GSA access.* The contractor shall afford GSA access to the contractor's and subcontractors' facilities, installations, operations, documentation, databases, IT systems and devices, and personnel used in performance of the contract, regardless of the location. Access shall be provided to the extent required, in GSA's judgment, to conduct an inspection, evaluation, investigation or audit, including vulnerability testing to safeguard against threats and hazards to the integrity, availability and confidentiality of GSA data or to the function of information technology systems operated on behalf of GSA, and to preserve evidence of computer crime. This information shall be available to GSA upon request.

(l) *Subcontracts.* The contractor shall incorporate the substance of this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(m) *Notification regarding employees.* The contractor shall immediately notify the contracting officer when an employee either begins or terminates employment when that employee has access to GSA information systems or data. If an employee's

employment is terminated, for any reason, access to GSA's information systems or data shall be immediately disabled and the credentials used to access the information systems or data shall be immediately confiscated.

(n) *Termination.* Failure on the part of the contractor to comply with the terms of this clause may result in termination of this contract.

(End of clause)

I.13 GSAM 552.246-77 Additional Contract Warranty Provisions for Supplies of a Noncomplex Nature (June 2009)

(a) Definitions. Correction, as used in this clause, means the elimination of a defect.

(b) Contractor's obligations. When return, correction, or replacement is required, the contractor shall be responsible for all costs attendant to the return, correction, or replacement of the nonconforming supplies. Any removal in connection with the above shall be done by the contractor at its expense.

(c) Remedies available to the government. When the nature of the defect in the nonconforming item is such that the defect affects an entire batch or lot of material, then the equitable price adjustment shall apply to the entire batch or lot of material from which the nonconforming item was taken.

(End of clause)

I.14 GSAM 552.252-6 Authorized Deviations in Clauses (SEP 1999)

(a) *Deviations to FAR clauses*.

(1) This solicitation or contract indicates any authorized deviation to a Federal Acquisition Regulation (48 CFR Chapter 1) clause by the addition of "(DEVIATION)" after the date of the clause, if the clause is not published in the General Services Administration Acquisition Regulation (48 CFR Chapter 5).

(2) This solicitation indicates any authorized deviation to a Federal Acquisition Regulation (FAR) clause that is published in the General Services Administration Acquisition Regulation by the addition of "(DEVIATION (FAR clause no.))" after the date of the clause.

(b) *Deviations to GSAR clauses*. This solicitation indicates any authorized deviation to a General Services Administration Acquisition Regulation clause by the addition of "(DEVIATION)" after the date of the clause.

(c) *"Substantially the same as" clauses*. Changes in wording of clauses prescribed for use on a "substantially the same as" basis are not considered deviations.

(End of clause)

(END OF SECTION I)

Enterprise Infrastructure Solutions (EIS)

Contract

Section J

List of Attachments

Issued by:

General Services Administration

Office of Information Technology Category

[redacted]

~~June~~ ~~2018~~January 2019

Table of Contents


GSA

J.1 Geographic Coverage

This Attachment specifies the geographic coverage requirements. The contractor shall provide and price mandatory services as specified in the Traffic Model. Geographic coverage requirements for service may differ between domestic and non-domestic areas. The Glossary (Attachment J.12) defines domestic and non-domestic areas.

J.1.1 Domestic Service Coverage

This section describes geographic coverage requirements for domestic areas for Core Based Statistical Area (CBSA) -based services, as defined in Table B.1.2.1.1. Non-CBSA-based services, as defined in Table B.1.2.1.1, do not have domestic coverage requirements. The contractor shall provide CBSA-based services at contractor POPs serving the locations indicated within a CBSA. Section J.1.3 describes the CBSA coverage requirements for access arrangements.

At a minimum, for each CONUS CBSA in which the contractor proposes prices, the contractor shall provide and price all mandatory CLINs for CBSA-based services to the following:

1. All NSCs in the Traffic Model[1] for that CBSA. For price tables with both originating and terminating location columns, Traffic Model records must be priced where the originating and terminating country/jurisdictions are both CONUS.
2. NSCs within that CBSA, beyond those contained in the Traffic Model, as requested by the government

For each OCONUS CBSA or OCONUS country/jurisdiction (that does not have a CBSA), where the contractor chooses to offer services, the contractor shall:

1. Propose prices for all the mandatory CLINs in the Traffic Model in the OCONUS CBSA or OCONUS country/jurisdiction chosen. For price tables with both originating and terminating location columns, a Traffic Model record must be priced if the OCONUS country/jurisdiction is present in the originating country/jurisdiction column and the terminating country/jurisdiction is either CONUS or the OCONUS country/jurisdiction.
2. Propose prices for all the mandatory CLINs in the OCONUS CBSA or OCONUS country/jurisdiction chosen, except as described in Table J.1.1.1. For those services in Table J.1.1.1, the contractor is only required to price the mandatory CLINs in the bandwidth (BW) ranges specified. For those services in Table

[1] The Traffic Model specifies a set of Network Site Codes, forms part of the minimum entry requirements, and is used for evaluation purposes.

J.1.1.1, mandatory scalable, bandwidth on demand, burstable and burstable overage CLINs are not required to be priced. For example, if the contractor chooses to price VPNS in an OCONUS country/jurisdiction, then the contractor shall price all the mandatory CLINs from VN00001 through VN00015 in that OCONUS country/jurisdiction.

Table J.1.1.1: ETS, IPS, VPNS, PLS CLIN Requirements for OCONUS country/jurisdictions

	ETS (E-LINE)	ETS (E-LAN Port)	IPS (Wireline)	IPS (Ethernet)	VPNS (Wireline)	VPNS (Ethernet)	PLS*
Min BW	10 Mbps	1 Mbps	T1	1 Mbps	T1	1 Mbps	DS0
Max BW	100 Mbps	100 Mbps	T3	100 Mbps	T3	100 Mbps	T3

* For PLS, the contractor shall, at a minimum, propose prices from CONUS to the country/jurisdiction chosen

In addition, for non-CBSA based services, the contractor shall provide and price services in the Traffic Model for all mandatory CLINs.

Contractors may propose a CBSA-based service for an OCONUS non-CBSA country/jurisdiction even if they do not propose any of the four mandatory services (VPNS, ETS, Voice, MNS) for that country/jurisdiction.

J.1.2 Non-Domestic Service Coverage

This section describes service coverage requirements for non-domestic areas.

Contractors may propose any CBSA-based service to a non-domestic area even if they do not propose any of the four mandatory services (VPNS, ETS, Voice, MNS) to that non-domestic area.

The Traffic Model contains specific services in non-domestic NSCs. For each country/jurisdiction where the contractor chooses to offer services, the contractor shall:

1. Propose prices for all the mandatory CLINs in the Traffic Model in the country/jurisdiction chosen, and
2. Propose prices for all the mandatory CLINs in the non-domestic country/jurisdiction chosen, except as described in Table J.1.2.A. For those services in Table J.1.2.A, the contractor is only required to price the mandatory CLINs in the bandwidth (BW) ranges specified. For those services in Table J.1.2.A, mandatory scalable, bandwidth on demand, burstable and burstable overage CLINs are not required to be priced. For example, if the contractor chooses to price VPNS in a non-domestic country/jurisdiction, then the contractor

shall price all the mandatory CLINs from VN00001 through VN00015 in that country/jurisdiction.

MTIPS is exempt from the requirements of J.1.2 (1) and J.1.2 (2) immediately above. Pricing of mandatory MTIPS CLINs is optional in non-domestic country/jurisdictions.

Table J.1.2.A: ETS, IPS, VPNS, PLS CLIN Requirements for Non-Domestic Country/Jurisdictions

	ETS (E-LINE)	ETS (E-LAN Port)	IPS (Wireline)	IPS (Ethernet)	VPNS (Wireline)	VPNS (Ethernet)	PLS*
Min BW	10 Mbps	1 Mbps	T1	1 Mbps	T1	1 Mbps	DS0
Max BW	100 Mbps	100 Mbps	T3	100 Mbps	T3	100 Mbps	T3

* For PLS, the contractor shall, at a minimum, propose prices from CONUS to the country/jurisdiction chosen

Non-domestic service is not required except as defined below. Table J.1.2.1 shows countries/jurisdictions where the contractor is required to support OCONUS and non-domestic off-net voice terminations for Internet Protocol Voice Service (IPVS), Circuit Switched Voice Service (CSVS) and Wireless Service (MWS). The contractor is also required to support IPVS and CSVS mobile terminations in the non-domestic countries/jurisdictions listed in Table J.1.2.1 except for satellite locations, which are the NONDOM locations in Table B.4.2.1 with no AOW ID.

J.1.2.1 OCONUS and Non-Domestic Countries/Jurisdictions Supporting Off-Net Voice Terminations and Non-Domestic Countries/Jurisdictions Supporting Mobile Voice Terminations Table

Country/Jurisdiction
Afghanistan
Albania
Algeria
Andorra
Angola
Anguilla
Antarctica
Antigua (includes Barbuda)
Argentina
Armenia
Aruba
Ascension Island
Australia

Country/Jurisdiction
Australian External Territory
Austria
Azerbaijan
Azores
Bahamas
Bahrain
Bangladesh
Barbados
Belarus
Belgium
Belize
Benin
Bermuda

Country/Jurisdiction
Bhutan
Bolivia
Bosnia - Herzegovina
Botswana
Brazil
British Indian Ocean Territories
British Virgin Islands
Brunei
Bulgaria
Burkina Faso
Burundi
Cambodia
Cameroon
Canada
Cape Verde Islands
Cayman Islands
Central African Republic
Chad
Chatham Island
Chile
China
Christmas Island
Cocos Islands
Colombia
Comoros
Congo, Dem. Republic Of The
Congo, Republic Of The
Cook Islands
Costa Rica
Cote d'Ivoire
Croatia
Cuba
Cyprus - North

Country/Jurisdiction
Cyprus - South
Czech Republic
Denmark
Diego Garcia
Djibouti
Domestic: Alaska
Domestic: American Samoa
Domestic: Commonwealth of Northern Marianas Islands (CNMI)
Domestic: Guam
Domestic: Hawaii
Domestic: Marshall Islands
Domestic: Micronesia
Domestic: Midway Island
Domestic: Palau
Domestic: Puerto Rico
Domestic: US Virgin Islands (USVI)
Domestic: Wake Island
Dominica
Dominican Republic
East Timor
Easter Island
Ecuador
Egypt
El Salvador
Equatorial Guinea
Eritrea
Estonia
Ethiopia
Faeroe Islands
Falkland Islands
Fiji Islands

Country/Jurisdiction
Finland
France
French Antilles
French Guiana
French Polynesia
French Southern Territory
Gabon
Gambia
Georgia
Germany
Ghana
Gibraltar
Global Sat
Greece
Greenland
Grenada
Guadeloupe
Guantanamo Bay
Guatemala
Guinea
Guinea - Bissau
Guyana
Haiti
Honduras
Hong Kong, Special Administrative District
Hungary
Iceland
India
Indonesia
Inmarsat Aero
Inmarsat Broadband Global Area Network (BGAN) I4-Americas
Inmarsat Broadband Global Area Network (BGAN) I4-Asia Pacific

Country/Jurisdiction
Inmarsat Broadband Global Area Network (BGAN) I4-EMEA (Europe, Middle East, Africa)
Inmarsat Fleet (Maritime) I4-Americas
Inmarsat Fleet (Maritime) I4-Asia Pacific
Inmarsat Fleet (Maritime) I4-EMEA (Europe, Middle East, Africa)
Inmarsat Global Express (GX) I5-AOR
Inmarsat Global Express (GX) I5-IOR
Inmarsat Global Express (GX) I5-POR
Inmarsat Mini-M
Inmarsat Swift (Aeronautical) Atlantic (AOR)
Inmarsat Swift (Aeronautical) Indian (IOR)
Inmarsat Swift (Aeronautical) Pacific (POR)
Iran
Iraq
Ireland
Iridium-8816
Iridium-8817
Israel
Italy
Jamaica
Japan (includes Okinawa)
Jordan
Kazakhstan
Kenya
Kiribati
Kosovo
Kuwait
Kyrgyzstan
Laos
Latvia
Lebanon
Lesotho

Country/Jurisdiction
Liberia
Libya
Liechtenstein
Lithuania
Luxembourg
Macau, Special Administrative District
Macedonia
Madagascar
Malawi
Malaysia
Maldives
Mali
Malta
Martinique
Mauritania
Mauritius
Mayotte Island
Mexico
Moldova
Monaco
Mongolia
Montenegro
Montserrat
Morocco
Mozambique
Myanmar
Namibia
Nauru
Nepal
Netherlands
Netherlands Antilles
Nevis
New Caledonia

Country/Jurisdiction
New Zealand
Nicaragua
Niger
Nigeria
Niue
Norfolk Island
North Korea
Norway (includes Svalbard)
Not Available
Oman
Pakistan
Palestinian Authority
Panama
Papua New Guinea
Paraguay
Peru
Philippines
Pitcairn Island
Poland
Portugal (includes Madeira)
Qatar
Reunion Island
Romania
Russia
Rwanda
Samoa
San Marino
Sao Tome
Saudi Arabia
Senegal
Serbia
Seychelles Islands
Sierra Leone

Country/Jurisdiction
Singapore
Slovakia
Slovenia
Solomon Islands
Somalia
South Africa
South Korea
South Sudan
Spain (includes Balearic Islands, Canary Islands, Ceuta and Malilla)
Sri Lanka
St. Helena
St. Kitts
St. Lucia
St. Pierre And Miquelon
St. Vincent And The Grenadines
Sudan
Suriname
Swaziland
Sweden
Switzerland
Syria
Taiwan
Tajikistan
Tanzania
Thailand
Thuraya Sat

Country/Jurisdiction
Togo
Tokelau
Tonga Islands
Trinidad And Tobago
Tunisia
Turkey
Turkmenistan
Turks And Caicos Islands
Tuvalu
Uganda
Ukraine
United Arab Emirates
United Kingdom
Uruguay
Uzbekistan
Vanuatu
Vatican City
Venezuela
Vietnam
Wallis And Futuna Islands
Western Sahara
Yemen
Zambia
Zanzibar (Province Of Tanzania)
Zimbabwe

J.1.3 Access Arrangement Coverage

This section defines access coverage requirements for both domestic and non-domestic areas.

J.1.3.1 Domestic Access Arrangement Coverage

This section defines access coverage requirements for domestic areas.

J.1.3.1.1 Access Arrangement

For the domestic CBSA regions CONUS, Alaska, Hawaii, and Puerto Rico, the contractor shall, at a minimum, provide access coverage and prices for the following:

1. All NSCs within a CBSA proposed as contained in the Traffic Model.
2. If an NSC has a wireline access CLIN other than OC-3c, E1 or E3 associated with it in the Traffic Model, then the contractor shall price all mandatory non-ICB wireline access CLINs, except OC-3c, E1 and E3 at that NSC (see Table B.2.9.1.5 for a list of mandatory non-ICB wireline access CLINs), and may optionally price the remaining access CLINs defined in B.2.9.1.5. If the wireline access CLIN in the Traffic Model is OC-3c, then the contractor shall price all mandatory non-ICB wireline access CLINs including OC-3c and excluding E1 and E3 at that NSC and may optionally price the remaining access CLINs defined in B.2.9.1.5. If the wireline access CLIN in the Traffic Model is E1, then the contractor shall price all mandatory non-ICB wireline access CLINs including E1 and excluding E3 and OC-3c at that NSC and may optionally price the remaining access CLINs defined in B.2.9.1.5. If the wireline access CLIN in the Traffic Model is E3, then the contractor shall price all mandatory non-ICB wireline access CLINs including E3 and excluding E1 and OC-3c at that NSC and may optionally price the remaining access CLINs defined in B.2.9.1.5.
3. If an NSC has an Ethernet access CLIN associated with it in the Traffic Model, then the contractor shall price all mandatory Ethernet access CLINs at that NSC (see table B.2.9.1.5 for a list of mandatory Ethernet access CLINs),and may optionally price the remaining access CLINs defined in B.2.9.1.5.
4. Additional NSCs beyond those contained in the Traffic Model, as requested by the government.

For domestic OCONUS non-CBSA regions, the contractor shall provide access coverage and prices for each NSC in the Traffic model within a proposed OCONUS region where the access CLIN is mandatory and is associated with a transport service that is offered in the OCONUS region.

The contractor shall provide switched access at all NSCs as necessary to provide purchased end-to-end service. The price for switched access shall be included in the transport price for Voice Service, Toll Free Service and Circuit Switched Data Service in accordance with Section B.2 Pricing Tables. Switched access shall include, at a minimum, Telcordia Feature Group B/D (on-net and off-net) or equivalent.

J.1.3.2 Non-Domestic Access Arrangement Coverage

This section defines access coverage requirements for non-domestic areas.

J.1.3.2.1 Access Arrangements

For non-domestic NSCs, the contractor shall price mandatory access CLINs in the Traffic Model that are associated with transport services offered in that non-domestic country/jurisdiction. Post-award, contractors shall price access as required by the underlying transport requested.

The contractor is required to provide off-net termination at no additional cost in those jurisdictions where the contractor provides service.

J.1.4 Traffic Model and Core Based Statistical Areas

The Traffic Model will be available within the EIS AcquServe Portal. It will represent a forecast of services by location of the agencies' expected use of the EIS contract. The Traffic Model contains information such as Service ID, CLIN, Originating NSC, Terminating NSC, Quantity, Originating CBSA, and Terminating CBSA. Prices from the contractor's Section B price tables will be "multiplied" by the Traffic Model to determine the Total Evaluated CBSA Price (TECP) for each service within each CBSA.

A list of CBSAs, sorted in order based on the aggregated bandwidth requirements, will be available in the EIS AcquServe Portal. Table J.1.4.1 lists the top 100 CBSAs. An NSC is associated with a CBSA based on its county. For NSCs that do not fall into a CBSA naturally based on its county, the following methodology is used for the Traffic Model, and will be used post-award to associate an NSC with a CBSA.

If an NSC's county does not fall within a CBSA, then:

1. Find the county within a CBSA and within the same state that is closest to the county of that NSC.
2. Assign the NSC to that CBSA.

Note: Non-CBSA Counties are associated with the closest CBSA County within the same State, using GPS coordinates found in the 2010 U.S. Census National Counties Gazetteer file (https://www.census.gov/geo/maps-data/data/gazetteer2010.html).

J.1.4.1 Top 100 Government Bandwidth CBSAs Table

Rank	CBSA Name	CBSA Code	Equivalent Gbps
1	Washington-Arlington-Alexandria, DC-VA-MD-WV	47900	902
2	Baltimore-Columbia-Towson, MD	12580	441
3	Durham-Chapel Hill, NC	20500	162
4	Dallas-Fort Worth-Arlington, TX	19100	125

Rank	CBSA Name	CBSA Code	Equivalent Gbps
5	Chicago-Naperville-Elgin, IL-IN-WI	16980	112
6	San Jose-Sunnyvale-Santa Clara, CA	41940	108
7	Salt Lake City, UT	41620	106
8	Kansas City, MO-KS	28140	77
9	Atlanta-Sandy Springs-Roswell, GA	12060	74
10	Virginia Beach-Norfolk-Newport News, VA-NC	47260	73
11	St. Louis, MO-IL	41180	58
12	Nashville-Davidson--Murfreesboro--Franklin, TN	34980	48
13	Chattanooga, TN-GA	16860	43
14	Denver-Aurora-Lakewood, CO	19740	42
15	San Diego-Carlsbad, CA	41740	36
16	Philadelphia-Camden-Wilmington, PA-NJ-DE-MD	37980	36
17	New York-Newark-Jersey City, NY-NJ-PA	35620	34
18	Houston-The Woodlands-Sugar Land, TX	26420	32
19	Richmond, VA	40060	27
20	Memphis, TN-MS-AR	32820	27
21	Huntsville, AL	26620	26
22	Orlando-Kissimmee-Sanford, FL	36740	26
23	Gulfport-Biloxi-Pascagoula, MS	25060	25
24	Hagerstown-Martinsburg, MD-WV	25180	21
25	San Antonio-New Braunfels, TX	41700	21
26	Albuquerque, NM	10740	20
27	Miami-Fort Lauderdale-West Palm Beach, FL	33100	20
28	Los Angeles-Long Beach-Anaheim, CA	31080	19
29	San Francisco-Oakland-Hayward, CA	41860	18
30	Pittsburgh, PA	38300	17
31	Ogden-Clearfield, UT	36260	16
32	Augusta-Richmond County, GA-SC	12260	14
33	Shreveport-Bossier City, LA	43340	14
34	Detroit-Warren-Dearborn, MI	19820	13
35	Boston-Cambridge-Newton, MA-NH	14460	13

Rank	CBSA Name	CBSA Code	Equivalent Gbps
36	Cleveland-Elyria, OH	17460	13
37	Seattle-Tacoma-Bellevue, WA	42660	11
38	Little Rock-North Little Rock-Conway, AR	30780	10
39	Austin-Round Rock, TX	12420	10
40	Phoenix-Mesa-Scottsdale, AZ	38060	9
41	Parkersburg-Vienna, WV	37620	9
42	Oklahoma City, OK	36420	9
43	Clarksburg, WV	17220	9
44	California-Lexington Park, MD	15680	9
45	Fayetteville, NC	22180	8
46	Sacramento--Roseville--Arden-Arcade, CA	40900	8
47	Minneapolis-St. Paul-Bloomington, MN-WI	33460	8
48	Jacksonville, NC	27340	8
49	Louisville/Jefferson County, KY-IN	31140	7
50	Portland-Vancouver-Hillsboro, OR-WA	38900	7
51	Sioux Falls, SD	43620	7
52	Birmingham-Hoover, AL	13820	7
53	Columbia, SC	17900	6
54	Tampa-St. Petersburg-Clearwater, FL	45300	6
55	Knoxville, TN	28940	6
56	Palm Bay-Melbourne-Titusville, FL	37340	6
57	New Orleans-Metairie, LA	35380	6
58	Indianapolis-Carmel-Anderson, IN	26900	6
59	Columbus, OH	18140	6
60	Cincinnati, OH-KY-IN	17140	5
61	Charleston-North Charleston, SC	16700	5
62	Tulsa, OK	46140	5
63	Omaha-Council Bluffs, NE-IA	36540	5
64	Mobile, AL	33660	4
65	Riverside-San Bernardino-Ontario, CA	40140	4
66	Jackson, MS	27140	4

Rank	CBSA Name	CBSA Code	Equivalent Gbps
67	Fresno, CA	23420	4
68	Montgomery, AL	33860	4
69	Gainesville, FL	23540	4
70	Milwaukee-Waukesha-West Allis, WI	33340	4
71	Charlotte-Concord-Gastonia, NC-SC	16740	4
72	Dublin, GA	20140	4
73	Morgantown, WV	34060	4
74	Dayton, OH	19380	3
75	Pocatello, ID	38540	3
76	El Paso, TX	21340	3
77	Las Cruces, NM	29740	3
78	San Juan-Carolina-Caguas, PR	41980	3
79	Jacksonville, FL	27260	3
80	Charleston, WV	16620	3
81	Urban Honolulu, HI	46520	3
82	Tucson, AZ	46060	3
83	Colorado Springs, CO	17820	3
84	Buffalo-Cheektowaga-Niagara Falls, NY	15380	3
85	Battle Creek, MI	12980	3
86	Fort Collins, CO	22660	3
87	Albany-Schenectady-Troy, NY	10580	3
88	Atlantic City-Hammonton, NJ	12100	3
89	Elkins, WV	21180	3
90	Asheville, NC	11700	3
91	Johnson City, TN	27740	3
92	Roanoke, VA	40220	3
93	Ann Arbor, MI	11460	3
94	Cumberland, MD-WV	19060	3
95	Las Vegas-Henderson-Paradise, NV	29820	3
96	Killeen-Temple, TX	28660	3
97	Tuscaloosa, AL	46220	2

Rank	CBSA Name	CBSA Code	Equivalent Gbps
98	Anchorage, AK	11260	2
99	Warner Robins, GA	47580	2
100	Providence-Warwick, RI-MA	39300	2

J.2 Contractor Data Interaction Plan

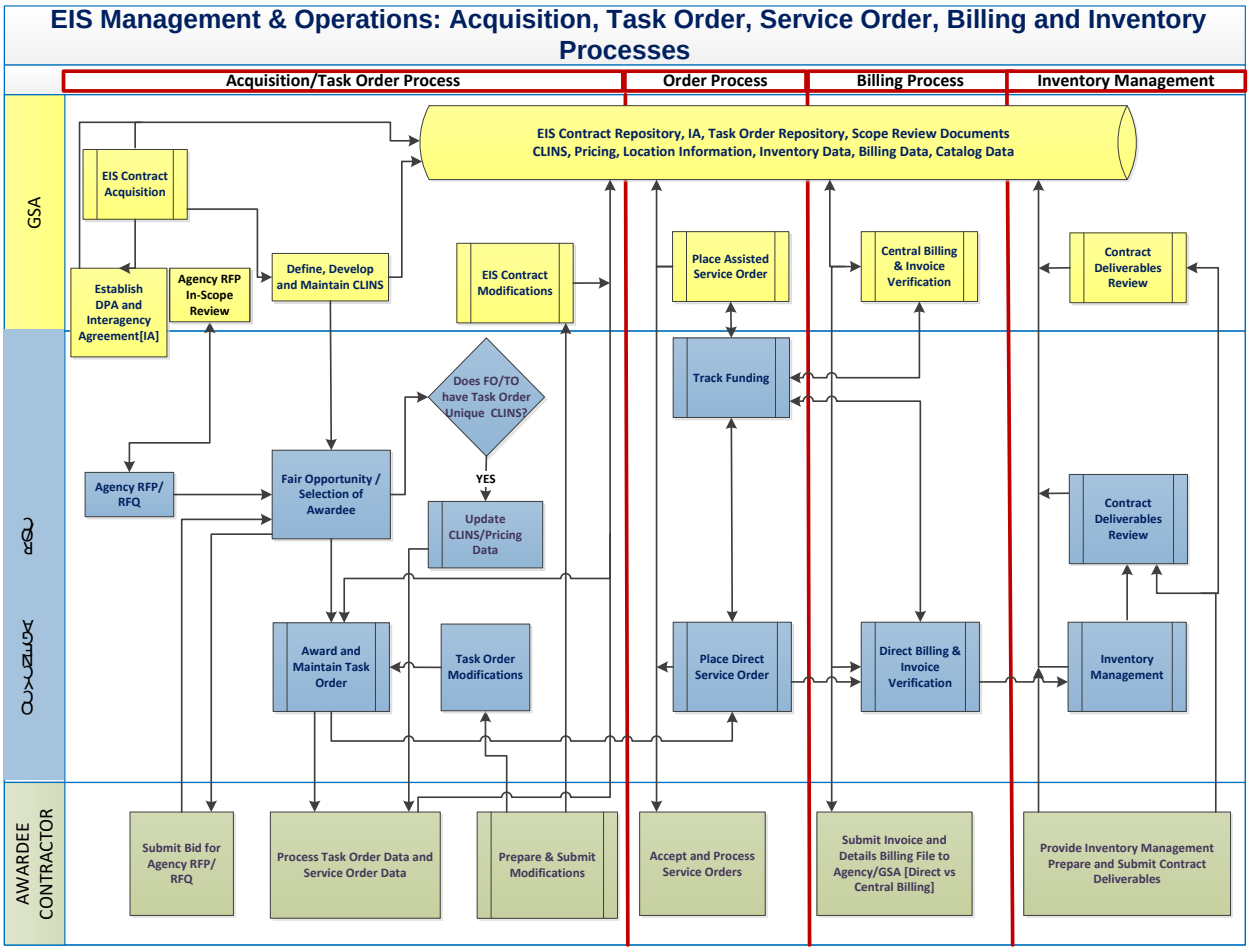
J.2.1 Introduction

This section details the requirements for common operations, process flows, data exchange details, and deliverables for various management and operation functions such as ordering, billing, inventory management, and SLA Management. It provides details on data interactions between the contractor, GSA and the customers. It includes requirements for direct interaction between GSA's next-generation network solutions management system (GSA Conexus), and the contractor's Business Support System (BSS) as described in Section G.5. It also includes requirements for contractor interaction with the set of tools used by GSA to manage the contract and TOs issued under the contract (GSA Systems).

For related management and operations functional requirements, see Section G Contract Administration Data.

The diagram in Section J.2.1.1 shows the high-level process flow relating to the acquisition/TO, ordering, billing and inventory management life cycle.

J.2.1.1 EIS Management and Operations: High-Level Process Diagram



J.2.1.2 Timeframes

Unless otherwise specified in the detailed requirements below, all timeframes in this Contractor Data Interaction Plan (CDIP) are in calendar days.

J.2.2 Common Data Interaction Requirements

J.2.2.1 Relevant Contracting Officer

Where permitted by the applicable section within the CDIP, exceptions to CDIP data submission requirements may be authorized, in writing, by the relevant Contracting Officer (CO). For these purposes, the relevant CO is defined as follows:

- For data submitted to GSA, the GSA CO is the relevant CO
- For data submitted to a customer, the Ordering Contracting Officer (OCO) is the relevant CO

J.2.2.2 Resubmission of Incorrect Deliverables

Unless specifically stated otherwise, if the contractor becomes aware of an error in a previously submitted deliverable, regardless of how it became aware of the error, the contractor shall:

1. Resubmit the deliverable within three (3) days of becoming aware of the error with the exception of billing errors identified after the government makes payment, which requires the submission of a billing adjustment as described in Section J.2.5 Billing.
2. Notify the relevant Contracting Officer's Representative (COR) and CO via email of the error and the action taken.

J.2.2.3 Deliverable Format, Content, and Transfer Mechanism

Unless otherwise specified, all contractor deliverables in the CDIP are governed by the following requirements:

- For deliverables submitted directly to GSA, including cases where GSA receives a copy of a deliverable sent to the customer, the contractor shall use the format, contents, and transfer mechanism specified herein unless an exception is authorized by the GSA CO (see also Section J.2.2.1 Relevant Contracting Officer and Section J.2.9 Data Transfer Mechanisms).
- For deliverables submitted directly to the customer, including cases where the customer receives a copy of a deliverable sent to GSA, the contractor may, with the approval of the OCO, use alternative formats, contents, and/or transfer mechanisms (see also Section J.2.2.1 Relevant Contracting Officer and Section J.2.9 Data Transfer Mechanisms). The TO may also specify alternative formats, contents, and/or transfer mechanisms for deliverables submitted to the customer.

J.2.2.4 Scope of Deliverables

Unless otherwise specified, the contractor shall submit all deliverables in accordance with the following deliverable scope requirements:

- The scope of all deliverables shall be at the TO level with each deliverable covering only a single TO.
- For deliverables submitted directly to GSA, including cases where GSA receives a copy of a deliverable sent to the customer, exceptions may be authorized by the GSA CO (see also Section J.2.2.1 Relevant Contracting Officer).
- For deliverables submitted directly to the customer, including cases where the customer receives a copy of a deliverable sent to GSA, exceptions may be authorized by the OCO or captured directly in the TO (see also Section J.2.2.1 Relevant Contracting Officer).

J.2.2.5 Empty Deliverables

Unless otherwise specified in the relevant contract section below or otherwise directed in accordance with Section J.2.2.3, the contractor shall submit all deliverables described in Section J.2 in accordance with the associated delivery timeframes even if the deliverable contains no data. If the deliverable is empty, i.e., it contains no data, the contractor shall submit a notice indicating that no data is available. Notwithstanding the delivery method indicated for the specific deliverable, this notice shall be sent via email to the GSA COR and, if the customer has previously requested receipt of the deliverable, to the customer OCO and COR. This notice is not required prior to the issuance of the first TO to the contractor.

J.2.3 Task Order Data Management

Task Order data management consists of initial setup and ongoing maintenance of TO data in GSA Conexus and the contractor's BSS. It begins immediately after the TO is issued (See Section G.3.2 Task Orders) and extends for the life of the TO.

TO data management covers three categories of data that GSA Conexus and the contractor's BSS require to allow effective data exchange between the contractor and the government.

1. **Task Order Controlled Data** – This data is contained in the TO or directly tied to it and can only change via a TO modification (See Section G.3). It includes, but is not limited to:
   - TO documents
   - TO-defined customer officials: OCO as defined Section G.2.2.1.1
   - Services specified on the TO
   - TO-Unique CLINs (TUCs) and Individual Case Basis (ICB) data
   - TO-unique Key Performance Indicators (KPIs) and Service Level Agreements (SLAs)
   - Other customer data specified on the TO
2. **Task Order Associated Data** – This data is not typically contained in the TO and can change at any time during the life of the TO. This data includes:
   - Additional TO Customer Officials not defined in the TO
   - Role-Based Access Control (RBAC) information
3. **System Reference Data** – These are universally applicable reference tables used to ensure both GSA Conexus and the contractor's BSS are using consistent codes for common transactional data. System reference data can only be modified by GSA. Examples include:

- Technical features such as Access Circuit Type and Bandwidth
- Business features such as Agency Bureau Codes and Dispute Reasons
- Status features such as Yes/No and True/False codes

J.2.3.1 Common Operational Requirements

The following are common operational requirements relating to contractor account management.

J.2.3.1.1 GSA Systems

GSA Systems is the set of tools used by GSA to manage the contract and TOs issued under the contract. The contractor shall submit data via GSA Systems as specified in Section J.2.3.2 Task Order Data Management Process.

J.2.3.1.2 Role-Based Access Control

As specified in Section G.5, the contractor shall provide Role-Based Access Control (RBAC) to allow only authorized users with appropriate permissions access to its BSS, including but not limited to, the ability to place orders and research order, billing, inventory, and performance information.

The contractor shall capture and store the authorized users for restricted access and restrict all information so that only the authorized users have access to this information. The contractor shall add new users within seven (7) days of customer request. The contractor shall remove any user who is no longer authorized within one (1) business day of notification or sooner if the situation requires.

J.2.3.2 Task Order Data Management Process

This section describes two TO data management processes for 1) System Reference Data and 2) Task Order Data. All deliverables and other data sets for these processes are further defined in Section J.2.3.3 Deliverables and Data Exchange.

J.2.3.2.1 System Reference Data

The contractor shall follow the process described below after the contractor's BSS has successfully completed verification and security testing as described in Section G.5 Business Support Systems and Section E.2.1 Business Support Systems Verification Testing, and as required by changes to the data. Changes may be caused by contract modifications and BSS changes approved by GSA in accordance with Section G.5. The contractor shall complete this process prior to setting up its first TO, as described in Section J.2.3.2.2 Task Order Data.

1. GSA will provide system reference data to the contractor using the data sets defined in Section J.2.3.3.1 Government-Provided Data: System Reference. GSA

will provide updates to the system reference data sets on an as needed basis. A contract modification will not be issued for such updates.

2. The contractor shall configure its BSS to submit data based on the provided system reference data.

J.2.3.2.2 Task Order Data

The contractor shall follow the process described below for each TO at initial TO setup prior to processing any orders for service as described in J.2.4 Ordering and as required by changes to the data. Changes may be caused by:

- Issuance of TO modifications
- New information from the customer (for data not defined in the TO)
- BSS changes approved by GSA in accordance with Section G.5
- Changes to the reference data as described in Section J.2.3.2.1

The contractor shall follow all process steps at initial setup of each TO, and shall complete this process prior to provisioning or providing any services under the TO.

Subsequent updates may omit submission of data sets where no changes have occurred unless directed otherwise by the GSA CO.

Process Steps:

1. The contractor shall submit the following deliverables to GSA:
   a) TO Services Awarded / TO CLINs Awarded
   b) TO Country/Jurisdiction Awarded By Service / TO Locations Awarded by Service
   c) TO Officials
   d) TO Customer Requirements Document Set
   e) TO Financials
   f) TO Key Performance Indicators
2. The contractor shall collect from the customer the list of users and user permissions for RBAC.
3. The contractor shall set up or modify appropriate RBAC permissions within its BSS as described in Section G.5 Business Support Systems.
4. The contractor shall submit the Direct Billed Agency Setup (DBAS) to GSA.

Updates to this data will follow the same process.

J.2.3.3 Deliverables and Data Exchange

J.2.3.3.1 Government-Provided Data: System Reference

The following table lists the reference data sets the government will provide as part of this process. Detailed contents of each data set are in Section J.2.10.2 Data Set Content. For each data set, the contractor shall support all required transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
Access Circuit Type	As required	Secure FTP
Access Framing	As required	Secure FTP
Access Jack Type	As required	Secure FTP
Access Provisioning	As required	Secure FTP
~~Account Type~~	~~As required~~	~~Secure FTP~~
Active Inactive	As required	Secure FTP
Adjustment Outcome	As required	Secure FTP
Adjustment Reason	As required	Secure FTP
Agency Bureau Code	As required	Secure FTP
Allowable Tax	As required	Secure FTP
Bandwidth	As required	Secure FTP
Charging Frequency	As required	Secure FTP
Charging Unit	As required	Secure FTP
Country	As required	Secure FTP
Data Transaction Type	As required	Secure FTP
~~Delivery Type~~	~~As required~~	~~Secure FTP~~
Dispute Reason	As required	Secure FTP
Dispute Status	As required	Secure FTP
KPI AQL Operator	As required	Secure FTP
KPI Location Qualifier	As required	Secure FTP
KPI Measurement Unit	As required	Secure FTP
KPI Service Level Qualifier	As required	Secure FTP
KPI Unit ~~Type~~Code	As required	Secure FTP
Line Coding	As required	Secure FTP
LOA Dependencies	As required	Secure FTP
Order Rejection	As required	Secure FTP

Data Set	Frequency	Transfer Mechanism
Order Type: Header Level	As required	Secure FTP
Order Type: Line Item Level	As required	Secure FTP
~~Primary Interexchange Carrier~~	~~As required~~	~~Secure FTP~~
Service	As required	Secure FTP
True/False	As required	Secure FTP
Yes/No	As required	Secure FTP

J.2.3.3.2 Reserved

J.2.3.3.3 Contractor-Provided Data Sets: Deliverables

The following table lists the deliverables the contractor shall provide as part of this process. Detailed contents of each data set are in Section J.2.10.2 Data Set Content. For each data set, the contractor shall support all required transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
TO CLINs Awarded	As required	Upload to GSA Systems
TO Country/Jurisdiction Awarded by Service	As required	Upload to GSA Systems
TO Officials	As required	Upload to GSA Systems
TO Customer Requirements Document Set	As required	Upload to GSA Systems
TO Financials	As required	Upload to GSA Systems
TO Key Performance Indicators	As required	Upload to GSA Systems
TO Locations Awarded by Service	As required	Upload to GSA Systems
TO Services Awarded	As required	Upload to GSA Systems
Direct Billed Agency Setup (DBAS)	As required	Web Services

J.2.4 Ordering

As described in Section G.3 Ordering, orders for service may be 1) defined in the TO, or 2) defined separately after the issuance of the TO.

J.2.4.1 Common Operational Requirements

J.2.4.1.1 Task Orders

The TO process is described in Section G.3 Ordering. Once a TO is issued, the contractor shall follow the process described in Section J.2.2.4 Task Order Data Management.

If the TO directly includes an order for services, the requirements and processes described in the remainder of this section (J.2.4 Ordering) apply to that order for service as well as to any subsequent orders for service under the TO.

If the TO does not directly include an order for services, the requirements and processes described in the remainder of this section (J.2.4 Ordering) do not apply to the processing of the TO, but do apply to all subsequent orders for service under the TO.

J.2.4.1.2 Agency Hierarchy Code

The Agency Hierarchy Code (AHC) is an internal government accounting code that shall be tracked for all services from order submission through disconnection. The government has the following AHC requirements for ordering:

1. An AHC is required on each line item in all orders.
2. The contractor shall validate the presence of an AHC on all order line items:
   a) The government will not pay for orders processed without an AHC on each line item
   b) The government does not require validation of the content of the AHCs unless specified on the TO
3. The contractor shall support AHC changes to provisioned services without an interruption of the associated service (see J.2.4.2.3 Administrative Change Orders).

J.2.4.1.3 Unique Billing Identifier

The Unique Billing Identifier (UBI) uniquely identifies one item or multiple items linked together for ordering, billing and inventory management purposes (see Section J.2.10.1.1.2 Unique Billing Identifier). The government has the following UBI requirements for ordering:

1. The contractor shall create the UBI as described in Section J.2.10.1.1.2.
2. The contractor shall provide the UBI as a data element in the Service Order Completion Notice (SOCN).

J.2.4.1.4 Agency Service Request Number

The Agency Service Request Number (ASRN) is an optional internal government control number that shall be tracked for all services from order submission through disconnection if it is provided. The government may elect to assign zero, one or two ASRNs to each line item in a given order. If the government provides ASRN data element(s) as part of a Service Order (SO), the contractor shall include them on all deliverables that reference that order or the services included in that order.

J.2.4.1.5 Contract Line Item Number

Each orderable element is identified by a Contract Line Item Number (CLIN), which may be associated with a case number. The government has the following CLIN requirements for ordering:

1. The contractor shall provide the CLIN and any associated ICB data element(s) for each line item in all ordering deliverables as required in Section J.2.4.3.2 Contractor Provided Data Sets: Deliverables.
2. The contractor shall ensure the CLINs reported on billing files match those included on the SOCN for a particular order.

J.2.4.1.6 Ordering Data Sets and Notices

The government and the contractor exchange several data sets as part of the ordering process.

- The delivery process, frequency, timing and detailed specifications for each are captured in subsequent sections.
- The TO can override the deliverable timing provided that both:
  - The notices remain in the order specified in the applicable process section under Section J.2.4.2 Ordering Process
  - All required notices are delivered prior to billing

The standard data sets are defined below:

- Service Order (SO): Provides the contractor with the required details of the government's order for service.
- Service Order Acknowledgement (SOA) Deliverable: Notifies the government its order for service has been received.
- Service Order Confirmation (SOC) Deliverable: Notifies the government that the order for service information is sufficient to process and has been issued.
- Service Order Rejection Notice (SORN) Deliverable: Notifies the government that the order for service information is insufficient or otherwise invalid and that the order cannot be processed.
- Firm Order Commitment Notice (FOCN) Deliverable: Notifies the government of the Firm Order Commitment (FOC) date when the contractor is committed to delivery of the ordered service.
- Service Order Completion Notice (SOCN) Deliverable: Notifies the government that service has been installed and/or activated (“turned up”). The order for service has been completed and billing starts as of the included completion date.

- Service Order Administrative Change (SOAC) Deliverable: Notifies the government that an administrative change has been completed and provides details of the change.
- Service State Change Notice (SSCN) Deliverable: Notifies the government that a UBI has changed state (e.g., an auto-sold CLIN has been activated).

J.2.4.1.7 Auto-Sold CLINs

In accordance with Section G.3.3.1.2 Auto-Sold CLINs, the government has the following auto-sold CLIN requirements for ordering:

1. The contractor shall include any auto-sold CLINs in all notices and deliverables that require reporting CLINs
2. Unless otherwise specified in the SO or TO, the contractor shall apply the AHC listed for the base CLIN to all associated auto-sold CLINs
3. Unless otherwise specified in the SO or TO, the contractor shall apply the ASRN(s) listed for the base CLIN to all associated auto-sold CLINs
4. The contractor shall manage activation and deactivation of auto-sold CLINs in accordance with Section J.2.4.1.10 Service State and Section J.2.4.2.5 Service State Changes

J.2.4.1.8 Order Types

Each order submitted by the customer will have an overall order type and each line item will have a line item order type. Order types are defined in Section J.2.10.1.1.4.

J.2.4.1.9 Splitting Complex Orders into Suborders

An order submitted by the customer may contain multiple line items for unrelated services, or otherwise require provisioning efforts that are not logically related. Upon confirmation of such an order, the contractor may split the order into logical suborders using its standard provisioning process with the following restrictions:

1. If the contractor splits an order such that separate suborders are used to provision services logically linked by a Service Grouping ID as described in Section J.2.10.1.1.2 Unique Billing Identifier, each such suborder shall have the same service order completion date reported in the associated SOCN~~Services logically linked by a Service Grouping ID as described in Section J.2.10.1.1.2 Unique Billing Identifier, shall not be split across multiple suborders~~
2. The contractor shall not split any SO into suborders if the SO or the TO contains instructions prohibiting such splitting
3. ~~2.~~ Each suborder must be processed fully as described in Section J.2.4.2.1 including issuing all required ordering data sets with the exception of the SORN which can only apply to the original order as issued by the government.

J.2.4.1.10 Service State

Each provisioned service, defined by a single UBI, is always in one of the following states:

- Active:
  - The UBI is active with charges accumulating
  - Other than auto-sold and band-priced CLINs, most UBIs will be in this state from provisioning to disconnection
  - Other than auto-sold, usage-priced CLINs are in this state if available for use
- Inactive:
  - The UBI is inactive with no charges accumulating
  - Does not apply to disconnected services
- Band_Name:
  - Only valid for UBIs based on band-priced CLINs
  - The band-priced UBI is in the band listed
  - The value to be provided as the UBI state is defined by combining the Band Low and Band High values from the associated Section B table separated by a single colon. For example, if the Band Low value is 10 and the Band High value is 100, the UBI state is 10:100.

The government has the following Service State requirements:

1. The contractor shall ensure that all provisioned UBIs have a valid service state assigned at all times:
   a) A UBI is not considered provisioned prior to the SOCN for its installation
   b) A UBI is not considered provisioned after the SOCN for its disconnection
2. The contractor shall not change the service state of a UBI except in response to direct government action (e.g., beginning or ending the use of an auto-sold CLIN) or as required based on predefined criteria captured in the contract or the TO.
3. Other than cloud services, a UBI based on a CLIN that is both auto-sold and usage-priced shall be in an Active state from its first use in a billing period until the end of the billing period.

See also Section B.1.2.11 Auto-Sold CLINs and Section B.1.2.4 Price Banding Structures.

J.2.4.2 Ordering Process

All deliverables and other data sets included in the processes below are defined in Section J.2.4.3 Deliverables and Data Exchange. Unless otherwise specified, the

contractor shall submit all deliverables in the process below to GSA and, if requested, to the customer.

J.2.4.2.1 Standard Orders

Standard orders, including moves, adds, changes (excluding administrative change orders), and disconnect orders, shall follow the process below (order updates are addressed in Section J.2.4.2.6):

1. The government will issue an SO.
2. The contractor shall submit an SOA within one (1) business day of SO.
3. If the contractor determines that the SO is invalid, the contractor shall submit a SORN within five (5) days of SO:
   a) A SORN submitted by the contractor shall apply to the entire order (i.e., the contractor may only reject entire orders, not individual line items)
   b) In the event of order rejection, the government may issue a new SO with the corrected information and restart this process
4. If the contractor determines that the SO is valid, it shall submit a SOC within five (5) days of SO.
5. The government may modify or cancel the order during the provisioning process as described in Section J.2.4.2.6 (see also Section J.2.10.1.1.4.3 and Section G.3.3.2.3).
6. If the contractor chooses to split a complex SO into suborders as described in Section J.2.4.1.9, the contractor shall follow the remainder of this process for each suborder including submitting separate deliverables for each suborder.
7. If the contractor must obtain local access services, the contractor shall submit a FOCN indicating its FOC date within one (1) business day of receiving the FOC date from the local provider.
8. If the contractor does not need to obtain local access services, the contractor shall submit a FOCN indicating its FOC date NLT the earlier of: 1) 5 days after SOC, or 2) 10 days before the FOC date.
9. Upon completion of the order, the contractor shall submit a SOCN within three (3) days of installation and testing unless otherwise specified in the TO.
10. If the government reports a problem within the acceptance period defined in Section E, Inspection and Acceptance (or as specified in the TO), the contractor shall fix, test, and submit a new SOCN.

J.2.4.2.2 Telecommunications Service Priority Orders

If the government submits a Telecommunications Service Priority (TSP) order as described in Section G.3.3.3.1 Telecommunications Service Priority Orders, the standard process (see Section J.2.4.2.1) shall apply with the following caveats:

1. The contractor shall follow the prioritizations applicable to TSP orders as noted in Section G.3.3.3.1 Telecommunications Service Priority Orders and/or Section G.11 National Security and Emergency Preparedness.
2. The contractor shall not delay the delivery of services in any way based on the need to submit deliverables specified in this process.

J.2.4.2.3 Administrative Change Orders

Administrative data changes to previously provisioned services, as described in Section G.3.3.2.2.4 Administrative Change Orders, shall be handled based on the restrictions and process in the subsections below.

J.2.4.2.3.1 Administrative Change Restrictions

As described in Section G.3.3.2.2.4, administrative change orders may only modify inventory data points provided by the government that have no impact on service delivery or pricing. Only the following fields fall into this category by default:

- Agency Service Request Number 1
- Agency Service Request Number 2
- Agency Hierarchy Code

Additional data elements can be subject to administrative change orders on a contract-wide or case-by-case basis with the mutual agreement of the contractor and the GSA CO.

J.2.4.2.3.2 Administrative Change Order Process

Note: unless otherwise specified, the contractor shall submit all deliverables described in the process below to GSA and, if requested, to the customer:

1. The government will issue an Administrative Change Order specifying the inventory items to be changed and details of the change.
2. The contractor shall update its systems and submit a SOAC within seven (7) days of the Administrative Change Order.
3. Other order notices (SOA, SOC, FOCN, and SOCN) are not required.

J.2.4.2.4 Rapid Provisioning

Certain services lend themselves to rapid provisioning as described in Section G.3.3.3.2 Rapid Provisioning Orders. In these cases, the government has streamlined its required process.

Note: this section does not apply to the activation of auto-sold CLINs (see Section J.2.4.2.5 Service State Changes).

Subject to the restrictions described in Section G.3.3.3.2, the contractor shall follow the standard process (Section J.2.4.2.1) with the following changes:

1. The SOC and the FOCN are not required.
2. If the contractor completes the provisioning process and issues a SOCN within twenty-four (24) hours of order submission, the SOA is not required.
3. If the contractor rejects an order, the SORN must be issued prior to the end of the defined provisioning interval.
4. The government's option to modify or cancel the order during the provisioning process is subject to the restrictions noted in Section G.3.3.3.2 Rapid Provisioning Orders.

J.2.4.2.5 Service State Changes

If a service (defined by a single UBI) changes from one state to another (as defined in J.2.4.1.10 Service State), the contractor shall issue a SSCN based on the type of service:

- For cloud services, the SSCN shall be submitted within 24 hours of the state change.
- For all other services, the SSCN shall be submitted no later than five (5) business days prior to the submission of the Billing Invoice (BI) containing the associated charge.

The contractor may combine multiple notices as individual line items on a single SSCN provided all notices are submitted within the timeframe specified for the service type.

J.2.4.2.6 Supplements or Updates to In-Progress Orders

If it is necessary to supplement or update an in-progress order as described in Section G.3.3.2.3 Updates to In-Progress Orders, the government will issue a supplement SO (see also Section J.2.10.1.1.4.3). Note: Changing data explicitly included in a TO requires a TO modification, and cannot be done via this process (see Section G.3.2.2 Task Order Modification).

In such cases, the following process shall be used:

1. The government will issue a supplement SO.
2. The contractor shall submit an SOA in response to the supplement SO within one (1) business day:
   - The Contractor Service Request Number (CSRN) reported on the SOA shall be the same as that reported on the original order
   - Note: TSP (Section J.2.4.2.2) and Rapid Provisioning (Section J.2.4.2.4) orders may have shorter submission times as defined in the applicable section
3. If the contractor determines that the supplement SO is invalid, the contractor shall submit a SORN in response to the supplement SO within three (3) days of the supplement SO:
   - The CSRN reported on the SORN shall be the same as that reported on the original order
   - Note: TSP (Section J.2.4.2.2) and Rapid Provisioning (Section J.2.4.2.4) orders may have shorter submission times as defined in the applicable section
4. The contractor shall update the original order with the new data.
5. If any changes are required to data sets already submitted in response to the original order (e.g., SOC, FOCN), the contractor shall issue updated versions of those notices.
6. The contractor shall complete the provisioning of the original order with updated information as described in the applicable order process:
   - Section J.2.4.2.1 - Standard Orders
   - Section J.2.4.2.2 - Telecommunications Service Priority Orders
   - Section J.2.4.2.4 - Rapid Provisioning Orders

J.2.4.3 Deliverables and Data Exchange

J.2.4.3.1 Government-Provided Data Sets

The following table lists the data sets the government will provide as part of this process. Detailed contents of each data set are provided in Section J.2.10.2 Data Set Content. The contractor shall support all required transfer mechanisms for each data set as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
Service Order (SO)	As required	o Contractor's Web Interface o Email o Other means as per the TO

Data Set	Frequency	Transfer Mechanism
Administrative Change Order	As required	o Contractor's Web Interface o Email o Other means as per the TO

J.2.4.3.2 Contractor-Provided Data Sets

The following table lists the deliverables the contractor shall provide as part of this process. Detailed contents of each data set are provided in Section J.2.10.2 Data Set Content. The contractor shall support all required transfer mechanisms for each data set as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
Service Order Acknowledgement (SOA)	NLT one (1) business day after SO	o Web Services o Email (if requested by the customer) o Contractor's Web Interface o Other means as agreed or required in the TO
Service Order Rejection Notice (SORN)	NLT 5 days after SO	o Web Services o Email (if requested by the customer) o Contractor's Web Interface o Other means as agreed or required in the TO
Service Order Confirmation (SOC)	NLT 5 days after SO	o Web Services o Email (if requested by the customer) o Contractor's Web Interface o Other means as agreed or required in the TO
Firm Order Commitment Notice (FOCN)	Local access subcontractor required: o within one (1) business day of receiving FOC date Local access subcontractor not required: o NLT the earlier of 5 days after SOC or 10 days before the FOC date	o Web Services o Email (if requested by the customer) o Contractor's Web Interface o Other means as agreed or required in the TO

Data Set	Frequency	Transfer Mechanism
Service Order Completion Notice (SOCN)	NLT 3 days after service is installed and tested	o Web Services o Email (if requested by the customer) o Contractor's Web Interface o Other means as agreed or required in the TO
Service Order Administrative Change (SOAC)	NLT 7 days after Administrative Change Order	o Web Services o Email (if requested by the customer) o Contractor's Web Interface o Other means as agreed or required in the TO
Service State Change Notice (SSCN)	Cloud Services: • Within 24 hours of state change All other services: • NLT 5 business days prior to submission of associated BI	o Web Services o Email (if requested by the customer) o Contractor's Web Interface o Other means as agreed or required in the TO

J.2.5 Billing

Billing functional requirements are described in Section G.4 Billing.

J.2.5.1 Common Operational Requirements

J.2.5.1.1 Billing Cycle

The contractor shall comply with the government's defined billing cycle, which runs from the first through the last day of the calendar month. Proration for partial months is described below in Section J.2.5.1.5 Proration.

J.2.5.1.2 Unique Billing Identifier

The UBI uniquely identifies one item or multiple items linked together for ordering, billing and inventory management purposes. It is defined in Section J.2.10.1.1.2 Unique Billing Identifier. The contractor shall ensure the UBI reported on billing deliverables matches the UBI included on the SOCN for a particular element.

J.2.5.1.3 Contract Line Item Number

Each billable element is identified by a CLIN, which may be associated with a case number. The government has the following CLIN requirements for billing:

1. The contractor shall provide the CLIN and any associated ICB data element(s) for each line item in all billing deliverables (described below Section J.2.5.2 Billing Process).
2. The contractor shall ensure that the CLINs reported on billing deliverables match those included on the SOCN for a particular order.

J.2.5.1.4 Associated Government Fee

The Associated Government Fee (AGF) is the fee GSA charges other customers for its services in supporting this contract. It is defined, along with calculation methods, in Section J.2.10.1.1.1 Associated Government Fee. The government has the following AGF requirements for billing:

1. The contractor shall calculate the AGF as described in Section J.2.10.1.1.1.
2. The contractor shall provide the AGF as a data element in billing deliverables (described below in Section J.2.5.2 Billing Process).
3. For TOs set up with direct billing (see Section G.4.2 Billing Methods), the contractor shall collect the AGF on behalf of GSA and transfer funds as described in Section G.4.6 Associated Government Fee.

J.2.5.1.5 Proration

For services not delivered for the full calendar month billing cycle, the contractor shall apply the following proration requirements.

J.2.5.1.5.1 Proration Formula

The contractor shall support one or both of the following proration types:

1. Month-Length Proration, defined in Section J.2.5.1.5.1.1
2. Normalized 30-Day Month Proration, defined in Section J.2.5.1.5.1.2

The contractor shall indicate which proration type or types are supported in its proposal. The contractor shall also indicate the proposed proration type in its response to each customer agency solicitation.

If a contractor does not support the proration type specified on a customer TO solicitation, the contractor may respond to the solicitation provided it clearly indicates in its response that it does not currently support the requested proration type.

The contractor may add support for a previously unsupported proration type at any time without contract modification by following the BSS Change Control process in Section G.5.5.1. The contractor shall complete successful retesting of the BSS test cases associated with proration prior to billing.

J.2.5.1.5.1.1 Month-Length Proration

1. Calculate the Daily Charge: divide the Monthly Recurring Charge (MRC) by the number of days in the billing month to get the Daily Charge
   [Daily Charge] = MRC / [Days in Month]
2. Find the First Billable Day
   a. If the service and pricing to be prorated were in effect on the first day of the billing month, the First Billable Day is 1
   b. Otherwise, the First Billable Day is the day the service was installed or the day of the new pricing start (see Section J.2.5.1.5.2)
3. Find the Last Billable Day
   a. If the service and pricing to be prorated are in effect on the last day of the billing month, the Last Billable Day is equal to the number of days in the billing month
   b. Otherwise, the Last Billable Day is the day the service was disconnected or the day of the pricing end (see Section J.2.5.1.5.2)
4. Calculate the Billable Days: the number of billable days for the service and pricing to be prorated is equal to the Last Billable Day minus the First Billable Day plus 1
   [Billable Days] = [Last Billable Day] – [First Billable Day] + 1
   a. Example 1: New service installed on March 17th
      [Billable Days] = 31 [Last Billable Day] – 17 [First Billable Day] +1 = 15
   b. Example 2: Service disconnected on June 10th:
      [Billable Days] = 10 [Last Billable Day] – 1 [First Billable Day] + 1 = 10
   c. Example 3: Service installed May 3rd and disconnected May 27th
      [Billable Days] = 27 [Last Billable Day] – 3 [First Billable Day] + 1 = 25
5. The billable amount for the service in that month (base_line_item_price) is equal to the daily charge from step 1 multiplied by the billable days from step ~~2~~4:
   [Billable Amount] = [Daily Charge] x [Billable Days]

J.2.5.1.5.1.2 Normalized 30-Day Month Proration

1. Calculate the Daily Charge: divide the Monthly Recurring Charge (MRC) by the 30 to get the Daily Charge
   [Daily Charge] = MRC / 30
2. Find the First Billable Day
   a. If the service and pricing to be prorated were in effect on the first day of the billing month, the First Billable Day is 1
   b. Otherwise, the First Billable Day is the day the service was installed or the day of the new pricing start (see Section J.2.5.1.5.2)
3. Find the Last Billable Day
   a. If the service and pricing to be prorated are in effect on the last day of the billing month, the Last Billable Day is equal to the number of days in the billing month
   b. Otherwise, the Last Billable Day is the day the service was disconnected or the day of the pricing end (see Section J.2.5.1.5.2)

4. Calculate the Billable Days: the number of billable days for the service and pricing to be prorated is equal to the Last Billable Day minus the First Billable Day plus 1
   [Billable Days] = [Last Billable Day] – [First Billable Day] + 1
   a. Example 1: New service installed on March 17th
      [Billable Days] = 31 [Last Billable Day] – 17 [First Billable Day] +1 = 15
   b. Example 2: Service disconnected on June 10th:
      [Billable Days] = 10 [Last Billable Day] – 1 [First Billable Day] + 1 = 10
   c. Example 3: Service installed May 3rd and disconnected May 27th
      [Billable Days] = 27 [Last Billable Day] – 3 [First Billable Day] + 1 = 25
5. Note: If Billable Days from Step 2 is equal to or greater than 30, proration does not apply; the contractor shall bill the full MRC for that month.
6. The billable amount for the service in that month (base line item price) is equal to the daily charge from step 1 multiplied by the billable days from step ~~2~~4:
   [Billable Amount] = [Daily Charge] x [Billable Days]

J.2.5.1.5.2 Service Change Order Proration

A service change order may necessitate a price change during a billing cycle.

For the purposes of proration, the contractor shall follow the process below to calculate prorated billing:

1. Treat the change as two connected events:
   - A previous service price end
   - A new service price start
2. The new service price is assigned a start date equal to the change date.
3. The previous service price is assigned an end date one (1) day prior to the start date for the new service price.
4. Calculate the prorated billing amount for each service pricing (ended previous and started new) using the standard proration formula (see J.2.5.1.5.1).

J.2.5.1.6 Rounding

J.2.5.1.6.1 Rounding Requirements

The contractor shall comply with the following requirements for rounding:

1. The contractor shall store charges and use in all calculations six (6) decimal places for service price [Quantity x Unit Price], prorating, taxes, fees and surcharges.
   - When rounding is necessary to reach 6 decimal places, the contractor shall apply the rounding standards in Section J.2.5.1.6.2
2. When calculating summary data (including total cost), the contractor shall:

a) Total each of the cost components that comprise the service including CLIN unit price (prorating if applicable), taxes, fees, and surcharges
b) Add the charges at the service level while maintaining the full 6 decimal places

3. When totaling the entire submitted bill, the contractor shall:
   a) Add the individual 6-decimal place service charges
   b) Round the total 6-decimal place value to 2 decimal places using the rounding standards in Section J.2.5.1.6.2

J.2.5.1.6.2 Rounding Standards

The contractor shall comply with the following rounding standards:

1. Rounding to reach 6 decimal place values:
   a) Upward rounding shall occur when the 7th decimal place is 5 or higher.
   b) Downward rounding shall occur with the 7th decimal place is 4 or lower.
   c) For example: if a cost component is $1113.8870974, since the 7th decimal place is 4, the cost component will be rounded to $1113.887097.
2. Rounding to reach 2 decimal place values:
   a) Upward rounding will occur when the 3rd decimal place is 5 or higher.
   b) Downward rounding shall occur when the 3rd decimal place is 4 or lower.
   c) For example: if the total amount due was $8395.4681674, since the 3rd decimal place is 8, the calculated amount due would be $8395.47.

J.2.5.1.6.3 Rounding Example Table

CLIN	Pricing Category	Pricing Component	Unit Value	Qty	Cost of Each Pricing Component	Rounding Notes
	EIS Service	Voice Service	$500.567800	3	$1,501.703400	Rounding does not apply
	Government Fee	AGF	5.000000%		$75.085170	Rounding does not apply
	Taxes & Surcharges	Universal Service Fund	16.100000%		$241.774247	$241.7742474 rounded to six decimal places
		Number Portability	$2.150000		$2.150000	Rounding does not apply
		911	$14.950000		$14.950000	Rounding does not

CLIN	Pricing Category	Pricing Component	Unit Value	Qty	Cost of Each Pricing Component	Rounding Notes
						apply
Total EIS Service Cost [Total Service Cost + Fees + Surcharges]					**$1,835.662817**	Rounding does not apply
	EIS Service	DS3 Data Service: NRC (Installation)	$279.370000	5	$1,396.850000	Rounding does not apply
		DS3 Data Service: MRC	$1083.370000	5	$5,416.850000	Rounding does not apply
	Government Fee	AGF	5.000000%		$340.685000	Rounding does not apply
	Taxes & Surcharges	Local Surcharge	$36.750000		$36.750000	Rounding does not apply
Total EIS Service Cost [Total Service Cost + Fees + Surcharges]					**$7,191.135000**	Rounding does not apply
TOTAL BILLED					**$9,026.80**	$9026.797817 rounded to two decimal places

J.2.5.1.7 Taxes, Fees, and Surcharges

Detailed requirements for the handling of taxes, surcharges, and fees are provided in:

- Section G.4.11 Taxes, Fees and Surcharges
- Section H.14 State and Local Taxes
- Section H.23 Fees and Surcharges

The contractor shall comply with the following data requirements for taxes, fees and surcharges:

1. Taxes, fees and surcharges shall be applied to each applicable line item as an aggregated total per billing line item.
2. Contractors shall provide the detail composition of the aggregated taxes, fees and surcharges on the Tax Detail (TAX) deliverable.

The contractor shall not aggregate taxes, surcharges, and fees into any other data element unless the TO specifies such aggregation (fully-loaded pricing) as described in Sections H.14 and H.23.

J.2.5.1.8 Billing Level

The contractor shall submit billing deliverables as described in Section J.2.5.2, using a TO billing level where each deliverable covers only a single TO unless the TO specifies another billing level.

J.2.5.1.9 Billing Data Sets

Several data sets are exchanged between the government and the contractor as part of the ordering process. The delivery process, frequency, timing and detailed specifications for each are captured in J.2.5.2 Billing Process. The standard data sets are defined below:

- Billing Invoice (BI) Deliverable: Provides the government with the full details of the contractor's invoice for the billing period. The BI shall include all taxes, fees, and surcharges as described in Section J.2.5.1.7. It shall not include any credits or adjustments. The contents of the BI and the BA together are used to calculate the total amount due from the government.
- Billing Adjustment (BA) Deliverable: Provides the government with the full details of any credits and other adjustments to the contractor's invoice for the billing period. The contents of the BI and the BA together are used to calculate the total amount due from the government.
- Tax Detail (TAX) Deliverable: Provides the government with the full details of the taxes, fees, and surcharges included in contractor's invoice for the billing period
- AGF Detail (AGFD) Deliverable: Provides the government with the full details of the AGF collected by the contractor from direct billed customers for the billing period; as this data set is submitted to GSA only, it shall be submitted at a contract level with each submission covering all TOs
- AGF Electronic Funds Transfer Report (ATR) Deliverable: Notifies the government that the contractor has transferred the collected AGF via Electronic Funds Transfer (EFT); as this data set is submitted to GSA only, it shall be submitted at a contract level with each submission covering all TOs
- Monthly Billing Information Memorandum Deliverable: Provides the government with background information, as necessary, to explain any items in the contractor's invoice for the billing period that may be unclear based on the contents of the BI alone

J.2.5.2 Billing Process

The standard billing process described below is applicable to all TOs. All deliverables and other data sets included in the processes below are defined in Section J.2.5.3

Deliverables and Data Exchange. Unless otherwise specified, the contractor shall submit all deliverables in the process below to GSA and, if requested, to the customer.

1. NLT the 15th business day of each month, the contractor shall submit the following billing deliverables based on the billing levels defined in Section J.2.5.1.8:
   a) Billing Invoice (BI)
   b) Tax Detail (TAX) unless the TO specifies fully-loaded pricing (See Sections H.14 and H.23)
   c) Monthly Billing Information Memorandum (to customer only), if required to clarify any line items on the BI
   d) Billing Adjustment (BA), if applicable
2. NLT the 15th business day of each month, the contractor shall submit the following billing deliverables to GSA only based on the billing levels defined in Section J.2.5.1.8:
   a) AGF Detail (AGFD)
   b) AGF Electronic Funds Transfer Report (ATR)
3. If the government determines that the BI is valid in its entirety, it will pay the contractor in full, as specified in Section G.4.5 Payment of a Bill by the Government.
4. If the government determines that the BI is not valid, in whole or in part, it will:
   a) Initiate a billing dispute as specified in Section G.4.4 Disputes
   b) Enter the dispute process described in Section J.2.6 Disputes
   c) Withhold payment to the contractor, in whole or in part, as specified in Section G.4.4 Disputes and further clarified in Section H.32 Payments and Incorrectly Billed Items
5. If required to correct errors identified after payment, the contractor shall submit a BA. Note: this does not apply to errors that have resulted in disputes as described in Section J.2.6 Disputes.

J.2.5.3 Deliverables & Data Exchange

J.2.5.3.1 Government-Provided Data Sets

The government will not provide any data sets as part of this process.

J.2.5.3.2 Contractor-Provided Data Sets

The following table lists the deliverables the contractor shall provide as part of this process. Detailed contents of each set of data are in Section J.2.10.2 Data Set Content. For each data set, the contractor shall support all required transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
Billing Invoice (BI)	Monthly, NLT 15th business day	o Secure FTP o Email (if requested by the customer) o Contractor's Web Interface o Other means as agreed or required in the TO
Billing Adjustment (BA)	Monthly, NLT 15th business day (as needed)	o Secure FTP o Email (if requested by the customer) o Contractor's Web Interface o Other means as agreed or required in the TO
Tax Detail (TAX)	Monthly, NLT 15th business day	o Secure FTP
AGF Detail (AGFD)	Monthly, NLT 15th business day	o Secure FTP
AGF Electronic Funds Transfer Report (ATR)	Monthly, NLT 15th business day	o Secure FTP
Monthly Billing Information Memorandum	Monthly, NLT 15th business day (as needed)	o Email o Contractor's Web Interface o Other means as agreed or required in the TO

J.2.6 Disputes

Functional requirements for disputes are described in Section G.4.4 Disputes.

J.2.6.1 Common Operational Requirements

The dispute process shall apply under any of the following conditions:

- The government disputes the content of a BI or TAX submitted by the contractor (see Section J.2.5 Billing).
- The government disputes the content of an Inventory Reconciliation (IR) submitted by the contractor (see Section J.2.7 Inventory Management). Inventory disputes will only occur if the remedies in G.7.1.4.1 are not sufficient.
- The government disputes an SLA Credit Request (SLACR) Response submitted by the contractor (see Section J.2.8 SLA Management).

J.2.6.2 Dispute Process

All deliverables and other data sets included in the dispute process below are defined in Section J.2.6.3 Deliverables and Data Exchange. The contractor shall submit them to both the customer and to GSA:

1. If the government is opening the dispute, it will submit a Dispute data set.

2. The contractor shall work with the government to resolve the dispute as described in Section G.4.4 Disputes.
3. NLT the 15th business day of each month, the contractor shall submit a Dispute Report (DR) that captures the current status of each opened dispute.
4. If applicable, upon resolution, the contractor shall apply any credits on a BA within two (2) billing cycles.

J.2.6.3 Deliverables & Data Exchange

J.2.6.3.1 Government-Provided Data Sets

The following table lists the data sets the government will provide as part of this process. Detailed contents of each data set are in Section J.2.10.2 Data Set Content. For each data set, the contractor shall support all required transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
Dispute	As required	o Secure FTP o Email o Contractor's Web Interface o Other means as agreed or required in the TO

J.2.6.3.2 Contractor-Provided Data Sets

The following table lists the deliverables the contractor shall provide as part of this process. Detailed contents of each set of data are in Section J.2.10.2 Data Set Content. For each data set, the contractor shall support all required transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
Billing Adjustment (BA)	See Section J.2.5 Billing	o See Section J.2.5 Billing
Dispute Report (DR)	Monthly, NLT 15th business day	o Secure FTP o Email (if requested by the customer) o Contractor's Web Interface o Other means as agreed or required in the TO

J.2.7 Inventory Management

The inventory management functional requirements are described in Section G.7 Inventory Management.

J.2.7.1 Common Operational Requirements

J.2.7.1.1 GSA Conexus Inventory

The government intends to maintain a separate inventory based on input from the contractor. This system will be used to validate the contractor's inventory data.

J.2.7.1.2 Agency Hierarchy Code

The AHC must be tracked for all services from order through disconnection. The government has the following AHC requirements for inventory management:

1. The contractor shall support AHC changes without an interruption of service.
2. The contractor shall provide the AHC as a data element in the Inventory Reconciliation (IR) deliverable (see Section J.2.7.2 Inventory Management Process).

J.2.7.1.3 Unique Billing Identifier

The UBI uniquely identifies one or more items linked together for ordering, billing and inventory purposes. It is defined in Section J.2.10.1.1.2 Unique Billing Identifier. The contractor shall ensure the UBI reported on the IR matches the UBI included on the SOCN and BI for a particular element.

J.2.7.1.4 Reporting of Inventory Item UBIs

The inclusion of a UBI in the IR is dependent on the pricing mechanism of the inventory item it represents. A UBI representing an inventory priced as a Monthly Recurring Charge (MRC) or priced based on usage shall be included in the IR for the month of installation and all subsequent IRs through the IR for the month of disconnection. A UBI representing an inventory priced as a Non-Recurring Charge (NRC) shall be included in the IR for the month of installation and all subsequent IRs until the NRC is billed (i.e., included on the BI) but may be excluded from all IRs thereafter.

J.2.7.2 Inventory Management Process

Inventory management shall follow the process below. Unless otherwise specified, the contractor shall submit all deliverables in the process below to GSA and, if requested, to the customer. All deliverables and other data sets included in the process below are defined in Section J.2.7.3 Deliverables and Data Exchange.

1. The contractor shall submit an IR deliverable monthly, NLT the 15th day of the month.
2. If the contractor identifies a discrepancy in a previously submitted IR, it shall submit a corrected IR within 3 days of identifying the discrepancy.
3. If the government identifies a discrepancy in the IR, it will follow the dispute process (Section J.2.6 Disputes).

J.2.7.3 Deliverables & Data Exchange

J.2.7.3.1 Government-Provided Data Sets

The government will not provide any data sets as part of this process.

J.2.7.3.2 Contractor-Provided Data Sets

The following table lists the deliverables the contractor shall provide as part of this process. Detailed contents of each set of data are in Section J.2.10.2 Data Set Content. For each data set, the contractor shall support all required transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
Inventory Reconciliation (IR)	Monthly, NLT 15th day of month	o Secure FTP o Email (if requested by the customer) o Contractor's Web Interface o Other means as agreed or required in the TO

J.2.8 SLA Management

Functional requirements for SLA management are captured in Section G.8 Service Level Management.

J.2.8.1 Common Operational Requirements

J.2.8.1.1 SLA Measurement

The contractor shall proactively measure each applicable SLA in accordance with its definition, capturing its performance relative to each KPI associated with the SLA as described in Section G.8.3.1 Measurement.

J.2.8.1.2 SLA Credit Requests

In the event of a missed SLA, the government shall issue a credit request within six (6) months of the SLAR containing the SLA failure. The contractor shall review such requests and respond as indicated in Section G.8.4.1 Credit Management.

J.2.8.2 SLA Management Process

All deliverables and other data sets included in the processes below are defined in Section J.2.8.3 Deliverables and Data Exchange. Unless otherwise specified, the contractor shall submit all deliverables in the process below to GSA and, if requested, to the customer.

J.2.8.2.1 SLA Reporting Process

1. The contractor shall measure each KPI associated with each applicable SLA as described in Section G.8 Service Level Management.
2. The contractor shall submit a Service Level Agreement Report (SLAR), which captures its performance on all applicable SLAs and associated KPIs monthly, NLT the 15th day of the month.
3. The contractor shall submit supplementary reports quarterly:
   a) Trouble Management Performance Summary Report (see G.8.5.2.3)
   b) Trouble Management Incident Performance Report (see G.8.5.2.4)

J.2.8.2.2 SLA Credit Process

In accordance with Section G.8.4 SLA Credit Management Methodology, credits for failed SLAs are managed with the following process:

1. The government shall issue a SLA Credit Request (SLACR) within six (6) months of the SLAR containing the SLA failure.
2. The contractor shall submit a SLACR response within 30 days of the SLACR.
3. If the contractor accepts the government's finding, the credit shall be reflected on a BA within two (2) billing cycles of the SLACR response.
4. If the contractor disagrees with the government's finding, the government may use the dispute process as defined in Section G.4.4 Disputes and Section J.2.6 Disputes.

J.2.8.3 Deliverables and Data Exchange

J.2.8.3.1 Government-Provided Data Sets

The following table lists the data sets the government will provide as part of this process. Detailed contents of each data set are in Section J.2.10.2 Data Set Content. For each data set, the contractor shall support all defined transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
SLA Credit Request (SLACR)	As required, NLT six (6) months after the SLA failure	o Secure FTP o Email o SLACR form (see SLACR description in Section J.2.10.2) o Other means as agreed or required in the TO

J.2.8.3.2 Contractor-Provided Data Sets

The following table lists the deliverables the contractor shall provide as part of this process. Detailed contents of each set of data are in Section J.2.10.2 Data Set Content. For each data set, the contractor shall support all required transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
Service Level Agreement Report (SLAR)	Monthly, NLT 15th day of month	o Secure FTP o Email (if requested by the customer) o Other means as agreed or required in the TO
SLA Credit Request Response	Within 30 days of SLACR	o Email o Other means as agreed or required in the TO
Trouble Management Performance Summary Report	Quarterly, NLT 14 days after the end of the FY quarter	o Email o Other means as agreed or required in the TO
Trouble Management Incident Performance Report	Quarterly, NLT 14 days after the end of the FY quarter	o Email o Other means as agreed or required in the TO
Billing Adjustment (BA)	See Section J.2.5 Billing	o See Section J.2.5 Billing

J.2.9 Data Transfer Mechanisms

The contractor shall support all data transfer mechanisms required for each data set.

J.2.9.1 Common Operational Requirements

J.2.9.1.1 Governance of Exceptions

Exceptions to the data transfer mechanisms and associated requirements described below may only be authorized by the relevant CO (see Section J.2.2.1 Relevant Contracting Officer).

J.2.9.1.2 Multiple Transfer Mechanisms

The contractor shall maintain the capability to accept all required data transfer mechanisms for data sets transferred from the government to the contractor.

The contractor shall submit data to the government using the listed data transfer mechanisms unless an exception is approved by the relevant CO.

J.2.9.2 Direct Data Exchange

J.2.9.2.1 Direct Data Exchange Mechanisms

The contractor shall support direct data exchange between its BSS and GSA Conexus based on the requirements captured in Section G.5.3.2 Direct Data Exchange using the following methods:

- Web Services: Extensible Markup Language (XML) over secure hypertext transfer protocol (HTTPS) using SOAP (formerly Simple Object Access Protocol) and applying commercial practices and standards
- Secure File Transfer Protocol (SFTP): Pipe-Separated Value (PSV) exchanged via a server operated by or on behalf of GSA

J.2.9.2.2 Attachments via Direct Data Exchange

The contractor shall also submit any Binary Large Object (BLOB) attachments required in the definitions of the various data sets in Section J.2.10.2. The contractor shall transfer these files separately via SFTP as described above and name the files based on the following template:

- CTRPREFIX-DTT-SEQNUM-ELEMENT.EXT

Each part of this filename template is defined below:

- CTRPREFIX = Code that uniquely identifies the contractor:
  - Chosen by the contractor
  - Registered by contractor during BSS testing with GSA approval to ensure uniqueness
  - 3 – 10 characters in length
  - Standard English alphabet (A-Z and a-z) and numbers (0-9) only
- DTT = Data Transaction Code from the associated data set:
  - See Section J.2.10.1.1.5
- SEQNUM = Data Transaction Sequence Number from the associated data set:
  - See Section J.2.10.2 Data Set Content
- ELEMENT = Element name of the attachment:
  - For example, design_documents
  - The contractor may package and compress large files using ZIP format as described in the ZIP APPNOTE available from PKWARE at https://www.pkware.com/documents/casestudies/APPNOTE.TXT.
  - If multiple files are required for one data element, the contractor shall package and compress the files into one file using ZIP format as described above

- EXT = Standard file extension based on file type:
  - For example, Microsoft Word files end in “doc” or “docx”
- Each component of the filename is separated by a single dash, “-” with the exception of the extension, which is separated by a single period, “.”

Example: ABC-SOCN-0837654-design_documents.zip would indicate that the contractor:

- Had registered the prefix ABC
- Was submitting this file as part of a Service Order Completion Notice (SOCN)
- Had given the SOCN in question the sequence number 0837654
- Was submitting this file as the design_documents data element
- Had packaged one or more files in a ZIP container

Note: The contractor shall not submit attachments with filenames that are not fully compliant with the specified template except as authorized in Section J.2.9.1.1 Governance of Exceptions.

J.2.9.3 Contractor’s Web Interface

Requirements for data transfer via the contractor's web interface are provided in Section G.5.3.1 Web Interface.

J.2.9.4 Email

Email is specified as the data transfer mechanism in cases where the data is unstructured or not intended for automated analysis. Data emailed from the government to the contractor may be included in the body of the email or in one or more attachments.

When emailing data to the government, the contractor shall:

1. Use body text only for brief information (not to exceed 150 words).
2. Use attachments for longer data sets or for structured data.
3. Use attachment formats that are compatible with one of the following.
   a) Microsoft Office (current version and two most recent prior versions)
   b) Portable Document Format (PDF)
   c) Other formats as approved in writing by the relevant CO
4. Encrypt attachments if required by the TO or the relevant CO.
5. Include appropriate contract and TO identification information in the body and all attachments.
6. Submit directly to the Point of Contact (POC) specified by the OCO.

J.2.9.5 GSA Systems

GSA Systems is the set of tools used by GSA to manage the contract and TOs issued under the contract. Data submitted to GSA Systems shall be submitted as uploaded files in either: 1) the original format of the document, or 2) in Comma-Separated Value (CSV) format, as defined for each deliverable specified as submitted via GSA Systems in Section J.2.10.2.

J.2.9.6 Other Means as Agreed or Required in the TO

The use of other means to transfer data must be approved in writing by the relevant CO or included in the TO.

J.2.10 Data Dictionary

J.2.10.1 Common Data Requirements

J.2.10.1.1 Extended Data Element Definitions

All data elements are defined with technical specifications in Section J.2.10.3 Data Element Specifications. However, a few data elements require more detailed explanations and definitions. Those elements are defined in the subsections below.

J.2.10.1.1.1 Associated Government Fee

The Associated Government Fee (AGF) is a government management service fee paid to GSA for management and support services. For direct-billed customers, on a monthly basis the contractor shall collect the AGF from the customer and remit to GSA as described in Section G.4.6 Associated Government Fee (AGF).

J.2.10.1.1.1.1 AGF Rate Structure

The AGF rate structure is governed by the following:

1. The AGF rate will be the same for all TOs under this contract
2. The AGF rate may change during the period of performance of this contract
3. The GSA CO will provide the contractor with notice of any changes to the AGF rate at least 30 days prior to the effective date of the new rate

J.2.10.1.1.1.2 AGF Calculation

The AGF is calculated using the following process:

1. Calculate the total revenue subject to AGF:
   a) If the TO specifies fully-loaded pricing as described in Sections H.14 and H.23, use the contractor's total billed revenue
   b) In all other cases, subtract all taxes, fees and surcharges from the contractor's total billed revenue

2. Multiply the result from Step 1 by the AGF rate provided by the government

J.2.10.1.1.2 Unique Billing Identifier

The UBI is a contractor-assigned code that uniquely identifies a group of related services for ordering, billing, and inventory purposes and also uniquely identifies each component within that grouping. A group of services may include one or more related services.

J.2.10.1.1.2.1 UBI Specifications

The UBI consists of two substrings separated by an underscore, "_":

1. Service Grouping ID: This value is unique to the grouping of services. It is shared by all components of the group but never reused for another group.
2. Component ID: This value is unique to each component within the group. It shall not be reused within the group but is not necessarily unique across groups.

Detailed field specifications for the UBI are included in Section J.2.10.3.1 Primary Data Element Dictionary. The contractor shall provide the UBI in accordance with those specifications and the following requirements:

- The complete UBI shall contain only the single prescribed underscore
- The complete UBI shall be unique across the contract and shall never be reused

Provided all other UBI requirements are met, the contractor may:

- Use existing fields in its system to capture the Service Grouping ID and the Component ID provided they are concatenated as described above on submission
- Determine the form of the Service Group ID and Component ID

J.2.10.1.1.2.2 UBI Process Requirements

1. The contractor shall create and assign the UBI for each installed service instance in compliance with the UBI Specifications described above, even if there is only one member of the service grouping.
   - Installed Service Instance Definition: a unique installation of a particular CLIN (or CLIN + ICB Case Number combination, if applicable)
   - For SRE, the UBI is assigned as above with each associated SRE Pricing Element using the same UBI (see also Section B.2.10)

2. The contractor shall provide the UBI to the government as part of the SOCN (see Section J.2.4 Ordering) and all other deliverables where it is a listed data element as specified in Section J.2.10.2 Data Set Content.
3. For auto-sold CLINs and CLIN bundling (see Section B.1.2.12), the contractor shall assign UBIs to the base CLIN (including TUCs), and to each associated auto-sold or component CLIN, and ensure the service grouping is the same on each.
4. The contractor shall maintain the UBI assignment for the duration of the contract even if the service is later disconnected.
5. The contractor shall apply logical grouping when constructing the service grouping such that services ordered and used together or otherwise interdependent shall be grouped together (e.g., a circuit with originating and terminating ends and equipment at each end shall all be included in the same service grouping). This requirement may be satisfied by, at minimum, ensuring the same service grouping is used for all UBIs representing CLINs for the same instance of a single service as defined in Section C.1.8.1.

J.2.10.1.1.3 Network Site Code

To specify locations under this contract, the government requires the use of Network Site Codes (NSCs), taken from the iconectiv Central Location Online Entry System (CLONES) database. The NSC uses geographical and geopolitical codes to represent buildings, structures, enclosures or other fixed, physical locations. The NSC has eight alphanumeric characters. The first four are the geographical representation of the city, the next two are the geopolitical representation of the state or country, and the final two represent the building associated with that geographical/geopolitical pair.

To support this requirement, the contractor shall:

1. Obtain access to the iconectiv CLONES database if the contractor does not already have such access. Although such access is required to support this contract, the government will not reimburse for contractor access to the database. The contractor shall be solely responsible for any charges incurred.
2. Use the iconectiv CLONES database to derive the NSC for all locations associated with an order:
   a) For dedicated access circuits, the circuit terminating location shall be used to derive the NSC
   b) For installed Service Related Equipment (SRE), the physical location of the SRE shall be used to derive the NSC
   c) For all other cases, including those services with no originating or terminating location, the address of the customer representative accepting the service (typically a local point of contact) shall be used to derive the NSC

3. Request an NSC from the iconectiv CLONES provider if the NSC for the location does not exist in the iconectiv CLONES database.
4. Capture and store the NSC, billing, originating and terminating address information as applicable, and provide the same on all deliverables as specified in the deliverable content list.

J.2.10.1.1.4 Order Types

While Section J.2.4.2 defines ordering processes and Section G.3 defines ordering requirements, populating the order type data elements provides additional definition to ensure that customer needs are adequately and efficiently addressed. This section defines the order type codes supplied by the government to the contractor under specific circumstances.

The order type of an SO is defined at two levels:

1. Header Level (order_header_type_code) defines the overall order type for the entire SO and reflects the overall purpose of the SO
2. Line Item Level (order_item_type_code) defines the order type of the individual line item within the SO

J.2.10.1.1.4.1 Orders for New Services

Orders for new services are defined as orders for services (CLINs) that are not currently being provided and that would require a new line item on the Billing Invoice (BI). For orders for new services, the contractor shall assign order types as follows:

- Header Order Type = Install
- Line Item Order type = Add

J.2.10.1.1.4.2 Orders to Change Existing Services

J.2.10.1.1.4.2.1 Move Orders

Move orders are defined as orders that require the removal of an existing service and/or SRE from one location and the re-installation of the identical service and/or SRE at another location. For move orders, the contractor shall assign order types as follows:

- Header Order Type = Change
- Removal of the existing service:
  - Line Item Order type = Remove
- Re-installation of the same service at the new location:
  - Line Item Order type = Add

J.2.10.1.1.4.2.2 Change in Features

Feature change orders are defined as orders that require changes to the features of an existing service as described in Section B. They fall into two (2) categories:

1. Feature changes that require a change to the CLIN being billed
2. Feature changes that do not require a change to the CLIN being billed

For feature changes that require a CLIN change, the contractor shall assign order types as follows:

- Disconnection of existing features and CLINs:
  - Header Order Type = Change
  - Line Item Order type = Remove
- Installation of new features and CLINs:
  - Header Order Type = Change
  - Line Item Order type = Add

For feature changes that do not require a CLIN change, the contractor shall assign order types as follows:

- Feature additions:
  - Header Order Type = Change
  - Line Item Order type = Add
- Feature removals:
  - Header Order Type = Change
  - Line Item Order type = Remove

J.2.10.1.1.4.2.3 Configuration

Configuration orders are defined as orders that require changes in the configuration of an existing service without adding or removing CLINs or features. For configuration orders, the contractor shall assign order types as follows:

- Header Order Type = Change
- Line Item Order type = Configuration

J.2.10.1.1.4.2.4 Disconnect

Disconnect orders are defined as orders that require the removal of services (CLINs) currently being provided. For disconnect orders, the contractor shall assign order types as follows:

- Header Order Type = Disconnect
- Line Item Order type = Remove

J.2.10.1.1.4.2.5 Change in Administrative Data

Administrative change orders are defined as orders that only require changes to administrative data associated with an existing service (CLIN) as described in Section G.3.3.2.2.4. Administrative change orders are submitted using the Administrative Change Order data set and have a unique process (see Section J.2.4.2.3). For administrative change orders, the contractor shall assign order types as follows:

- Header Order Type = Change
- Line Item Order type = Administrative

J.2.10.1.1.4.2.6 Clarification of Line Items Being Changed

To clarify the order line items being changed, the government may include unchanged line items on the change SO using the following order types:

- Header Order Type = Change
- Line Item Order type = None

J.2.10.1.1.4.3 Orders to Supplement or Update In-Progress Orders

Within the limitations defined in Section G.3, SO line items that have not completed the provisioning process may be supplemented or updated by the government to accommodate the following situations:

1. Cancel the Order in whole or in part
2. Update Service Delivery Location
3. Update Service Features
4. Update the Customer Want Date (CWD)
5. Update Administrative Data

Note: The order types listed in this section are contained in the supplement SO. They do not reflect changes to the order type of the original SO being supplemented or updated.

J.2.10.1.1.4.3.1 Order Cancellation

Order cancellation updates are defined as order updates that cancel the original order in its entirety. For order cancellation updates, the contractor shall assign order types as follows:

- Header Order Type = Cancel
- Line Item Order type = Cancel

Note: if the order cancellation is issued beyond the deadlines specified in Section G.3.3.2.3.1 and a cancellation CLIN is applied, the order update is handled as described in Section J.2.10.1.1.4.3.2 Line Cancellation.

J.2.10.1.1.4.3.2 Line Cancellation

Line cancellation updates are defined as order updates that cancel the line item in the original order. For line cancellation updates, the contractor shall assign order types as follows:

- Header Order Type = Supplement
- Line Item Order type = Cancel

Note: if the line cancellation update is issued beyond the deadlines specified in Section G.3.3.2.3.1 and a cancellation CLIN is applied, the contractor shall assign the line item order type "Add" to the cancellation CLIN.

J.2.10.1.1.4.3.3 Update Specified Location

Location change updates are defined as order updates that change the specified service delivery location from that specified in the original order. They fall into two (2) categories:

1. Changes in service delivery location that have an impact on Local Exchange Carrier (LEC) provisioning
2. Changes in service delivery location that do not have an impact on LEC provisioning

For location change updates that have an impact on LEC provisioning, the contractor shall assign order types as follows:

- Cancelation of existing SO line item:
  - Header Order Type = Supplement
  - Line Item Order type = Cancel
- Corrected order with addition of new features and CLINs:
  - Header Order Type = Install
  - Line Item Order type = Add

For location change updates that do not have an impact on LEC provisioning, the contractor shall assign order types as follows:

- Header Order Type = Supplement
- Line Item Order type = Update

J.2.10.1.1.4.3.4 Update Specified Features

Feature change updates are defined as order updates that require changes to the features of an existing service. They fall into two (2) categories:

1. Feature changes that require a change to the CLIN originally ordered
2. Feature changes that do not require a change to the CLIN originally ordered

For feature changes that require a CLIN change, the contractor shall assign order types as follows:

- Cancel of original order features and CLINs:
  - Header Order Type = Supplement
  - Line Item Order type = Cancel
- Corrected order with addition of new features and CLINs:
  - Header Order Type = Install
  - Line Item Order type = Add

For feature changes that do not require a CLIN change, the contractor shall assign order types as follows:

- Header Order Type = Supplement
- Line Item Order type = Update

J.2.10.1.1.4.3.5 Update Specified Customer Want Date

Customer Want Date (CWD) updates are defined as order updates that change the customer want date from that specified in the original order. For CWD updates, the contractor shall assign order types as follows:

- Header Order Type = Supplement
- Line Item Order type = Update

J.2.10.1.1.4.3.6 Update Specified Administrative Data

Administrative data updates are defined as order updates that change the administrative data associated with an existing service (CLIN) as described in Section G.3.3.2.3.5 from that specified in the original order. For administrative data updates, the contractor shall assign order types as follows:

- Header Order Type = Supplement
- Line Item Order type = Update

J.2.10.1.1.4.3.7 Clarification of Line Items Being Updated

To clarify the order line items being updated, the government may include non-updated line items on the supplement SO using the following order types:

- Header Order Type = Supplement
- Line Item Order type = None

J.2.10.1.1.5 Data Transaction Code

Each data set exchanged between the contractor and GSA, regardless of direction, shall include an element labeled data_transaction_code. This code uniquely identifies the specific data set (i.e., it distinguishes a Billing Invoice from a Billing Adjustment). Unless otherwise specified, each data set defined in Section J.2.10.2 has a unique data transaction code included in its definition. The contractor shall include the correct code in each data set submitted to GSA as detailed in the data set definition.

J.2.10.1.2 Data Consistency

Unless otherwise specified, the contractor is free to format data according to its normal commercial practices. However, the contractor shall submit each data element in a consistent format. This includes, but is not limited to:

- Case sensitivity:
  - For example, "xml" is not the same as "XML"
- Punctuation and whitespace are treated as values:
  - For example, "x.m.l" is not the same as "x_m_l" or "x m l"
- Leading or trailing characters are part of the value:
  - For example, " xml" (leading space) is not the same as "xml" or ".xml"

J.2.10.1.3 Data Set Structure

J.2.10.1.3.1 GSA Systems CSV Structure

For all data sets submitted as CSV via GSA Systems, the data element order listed in Section J.2.10.2 shall be used in structuring the table (i.e., the column order of the submitted table shall match the specified field order). For data sets submitted with multiple rows of data, all data elements are included in each row even if unchanged from the previous row.

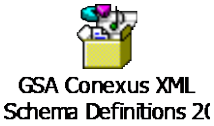
J.2.10.1.3.2 PSV Structure

For all data sets submitted using PSV over SFTP, the data element order listed in Section J.2.10.2 shall be used in structuring the PSV file (i.e., the column order of the submitted file shall match the specified field order). For data sets submitted with multiple rows of data, all data elements are included in each row even if unchanged from the previous row.

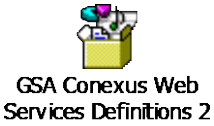
J.2.10.1.3.3 XML & Web Services Structure

For all data sets submitted using XML over Web Services, the data shall be structured in accordance with the applicable XML Schema Definitions (XSDs), Web Services Definition Language (WSDL) documents, and associated documents provided by GSA. The contractor shall use these schemas and documents in establishing Web Services connections with GSA Conexus.

J.2.10.1.3.3.1 GSA Conexus XML Schema Definitions



J.2.10.1.3.3.2 GSA Conexus Web Services Definitions



J.2.10.2 Data Set Content

The tables below detail the contents of each data set to be exchanged as part of the processes described throughout this CDIP. Unless otherwise stated, specific details of the format, limitations and definition of each data element are contained in Section 0 Data Element Specifications. The structure of the data submitted is defined in Section J.2.10.1.3 Data Set Structure.

The three subsections below address different groups of data sets:

- Section J.2.10.2.1 Data Sets: Primary Data:
  - Contains all data sets transacted as part of all CDIP processes except system reference data and TO data.
  - Element specifications are in Section J.2.10.3.1.2 Primary Data Element Dictionary unless otherwise specified.
- Section J.2.10.2.2 Data Sets: Reference Data:
  - Contains all reference data sets transacted as part of the CDIP processes defined in Section J.2.2.4 Task Order Data Management.
  - Element specifications are in Section J.2.10.3.2 Reference Data Element Dictionary unless otherwise specified.
- Section J.2.10.2.3 Data Sets: Task Order Data:
  - Contains all TO data sets transacted via GSA Systems as part of the CDIP processes defined in Section J.2.2.4 Task Order Data Management.
  - Element specifications are contained within the individual tables listed.

J.2.10.2.1 Data Sets: Primary Data

The columns of the tables in this section are defined below:

- Element Name:
  - The actual element name
    - For data sets transacted via Web Services, this is the data element name used in the xml file
    - For data sets transacted via secure FTP, this is the column heading (first row)
  - Used to locate the corresponding element specification in Section J.2.10.3 Data Element Specifications
- Value Requirement:
  - Indicates if the field must always have a valid value (that is, it must not be empty).
  - Contains one of the following which have specific defined meanings:
    - Always: The contractor shall supply the correct value for the element on all submissions.
    - If Applicable: The contractor shall supply the correct value for the element on all submissions where the value is applicable.
    - Either/Or: The contractor shall supply the correct value for only one of the data elements so labeled and shall apply the specific requirements for that data set in choosing which to supply.
  - Note: For data elements that do not have a required value under the rules above:
    - If the data set is transferred via Web Services, the data field may be omitted entirely
    - In all other cases, all data element fields are always required to be present even if empty
- Unique Value Level
  - Indicates if the value can vary with each line item in the data set, or if the data set is only permitted to have the same value for each line item
  - Contains one of the following values, which have specific defined meanings:
    - Data Set: Each data set contains only one unique value for this element. For data sets submitted in tabular format (e.g. PSV over secure FTP), each line item shall contain the same value for this data element.
    - Line Item: Each line item in the data set contains a unique value for this data element, which may or may not be the same as other line items in the data set.

- Note: This column is not included for all data sets. If the column is not included for a particular data set, all data elements in that data set may vary by line item.

J.2.10.2.1.1 Administrative Change Order

Data Transaction Code: SO

The administrative change order is a specific type of service order (see also Section J.2.10.2.1.15). Unless otherwise specified by the TO, the government may use a variety of structured or unstructured formats for this data set. In all cases, the data submitted by the government will contain sufficient data to:

- Uniquely identify the inventory/billing elements subject to change (e.g., UBI)
- Clearly communicate the administrative change required
- Provide contact information for the order (e.g., email address of the COR)

J.2.10.2.1.2 AGF Detail

Data Transaction Code: AGFD

Element Name	Value Requirement
data_transaction_code	Always
data_transaction_file_date	Always
contract_number	Always
contractor_invoice_number	Always
contractor_invoice_date	Always
billing_period	Always
contractor_direct_billed_agf_collected	Always
contractor_direct_billed_agf_adjustment	Always

J.2.10.2.1.3 AGF Electronic Funds Transfer Report

Data Transaction Code: ATR

Element Name	value requirement
data_transaction_code	always
data_transaction_file_date	always
contract_number	always
contractor_direct_billed_agf_collected	always
contractor_direct_billed_agf_adjustment	always
agf_electronic_funds_transfer_amount	always
agf_electronic_funds_transfer_date	always

J.2.10.2.1.4 Billing Adjustment

Data Transaction Code: BA

- Although specified as “If Applicable”, values are always required for “unique_billing_identifier” except for the Billing Data Accuracy KPI (see Section G.4.12.1) and the Billing Charges Accuracy KPI (see Section G.4.12.2).

Element Name	Value Requirement
data_transaction_code	Always
data_transaction_file_date	Always
contract_number	Always
contractor_service_request_number	If Applicable
contractor_invoice_level_account_number	Always
contractor_service_level_account_number	If Applicable
agency_task_order_num	Always
data_transaction_line_sequence_number	Always

Element Name	Value Requirement
agency_service_request_number_1	If Applicable
agency_service_request_number_2	If Applicable
unique_billing_identifier	If Applicable
agency_hierarchy_code	If Applicable
contract_line_item_number	If Applicable
clin_description	If Applicable
individual_case_basis_code_number	If Applicable
quantity	Always
fully_loaded_price_code	Always
charging_frequency_and_sre_element_code	If Applicable
charging_unit_code	If Applicable
base_line_item_price	If Applicable
iconectiv_nsc	If Applicable
terminating_iconectiv_nsc	If Applicable
contractor_invoice_number	Always
contractor_invoice_date	Always
billing_period	Always
billing_begin_date	Always
billing_end_date	Always
band_amount	If Applicable
service_connect_start_date_and_time	If Applicable
service_connect_end_date_and_time	If Applicable

Element Name	Value Requirement
billing_authorization_code	If Applicable
originating_number	If Applicable
originating_location_city	If Applicable
originating_location_state	If Applicable
originating_location_county	If Applicable
originating_location_country	If Applicable
originating_jurisdiction_code	If Applicable
terminating_number	If Applicable
terminating_location_city	If Applicable
terminating_location_state	If Applicable
terminating_location_county	If Applicable
terminating_location_country	If Applicable
terminating_jurisdiction_code	If Applicable
usage_event_id	If Applicable
billing_quantity	If Applicable
billing_reserved_01	If Applicable
billing_reserved_02	If Applicable
billing_reserved_03	If Applicable
billing_reserved_04	If Applicable
billing_reserved_05	If Applicable
billing_reserved_06	If Applicable
billing_reserved_07	If Applicable

Element Name	Value Requirement
billing_reserved_08	If Applicable
billing_reserved_09	If Applicable
billing_reserved_10	If Applicable
billing_reserved_11	If Applicable
billing_reserved_12	If Applicable
billing_reserved_13	If Applicable
billing_reserved_14	If Applicable
billing_reserved_15	If Applicable
agency_agf_percent_rate	Always
contractor_charge_waiver_code	If Applicable
total_line_item_amount	If Applicable
agf_amount	If Applicable
billed_aggregated_tax	If Applicable
line_net_amount	If Applicable
original_bill_line_item_sequence_number	If Applicable
original_bill_billing_period	Always
agency_dispute_number	If Applicable
contractor_dispute_number	If Applicable
adjustment_date	Always
adjustment_amount	Always
adjustment_aggregated_tax	Always
adjustment_detail_tax_billed	Always

Element Name	Value Requirement
adjustment_reason	Always
adjustment_outcome	Always
contractor_dispute_adjustment_comments	If Applicable
service	If Applicable
sla_item_identification	If Applicable
tax_item_number	If Applicable

J.2.10.2.1.5 Billing Invoice

Data Transaction Code: BI

Element Name	Value Requirement
data_transaction_code	Always
data_transaction_file_date	Always
contract_number	Always
contractor_service_request_number	Always
contractor_invoice_level_account_number	Always
contractor_service_level_account_number	Always
agency_task_order_num	Always
contracting_officer_representative_email_address	Always
service_order_completion_date	Always
data_transaction_line_sequence_number	Always
agency_service_request_number_1	If Applicable
agency_service_request_number_2	If Applicable

Element Name	Value Requirement
unique_billing_identifier	Always
agency_hierarchy_code	Always
contract_line_item_number	Always
clin_description	Always
individual_case_basis_code_number	If Applicable
~~Quantity~~quantity	Always
fully_loaded_price_code	Always
charging_frequency_and_sre_element_code	If Applicable
charging_unit_code	If Applicable
base_line_item_price	If Applicable
iconectiv_nsc	Always
terminating_iconectiv_nsc	If Applicable
building	If Applicable
bandwidth_code	If Applicable
billing_telephone_number	If Applicable
contractor_transport_circuit_number	If Applicable
phone_number_toll_free_and_700_number	If Applicable
card_number	If Applicable
alternate_code_description	If Applicable
directed_to_number	If Applicable
labor_email_address	If Applicable
body_detail_reserved_01	If Applicable

Element Name	Value Requirement
body_detail_reserved_02	If Applicable
body_detail_reserved_03	If Applicable
body_detail_reserved_04	If Applicable
body_detail_reserved_05	If Applicable
body_detail_reserved_06	If Applicable
body_detail_reserved_07	If Applicable
body_detail_reserved_08	If Applicable
body_detail_reserved_09	If Applicable
body_detail_reserved_10	If Applicable
body_detail_reserved_11	If Applicable
body_detail_reserved_12	If Applicable
body_detail_reserved_13	If Applicable
body_detail_reserved_14	If Applicable
body_detail_reserved_15	If Applicable
contractor_invoice_number	Always
contractor_invoice_date	Always
billing_period	Always
billing_begin_date	Always
billing_end_date	Always
band_amount	If Applicable
service_connect_start_date_and_time	If Applicable
service_connect_end_date_and_time	If Applicable

Element Name	Value Requirement
billing_authorization_code	If Applicable
originating_number	If Applicable
originating_location_city	If Applicable
originating_location_state	If Applicable
originating_location_county	If Applicable
originating_location_country	If Applicable
originating_jurisdiction_code	Always
terminating_number	If Applicable
terminating_location_city	If Applicable
terminating_location_state	If Applicable
terminating_location_county	If Applicable
terminating_location_country	If Applicable
terminating_jurisdiction_code	If Applicable
usage_event_id	If Applicable
billing_quantity	If Applicable
billing_reserved_01	If Applicable
billing_reserved_02	If Applicable
billing_reserved_03	If Applicable
billing_reserved_04	If Applicable
billing_reserved_05	If Applicable
billing_reserved_06	If Applicable
billing_reserved_07	If Applicable

Element Name	Value Requirement
billing_reserved_08	If Applicable
billing_reserved_09	If Applicable
billing_reserved_10	If Applicable
billing_reserved_11	If Applicable
billing_reserved_12	If Applicable
billing_reserved_13	If Applicable
billing_reserved_14	If Applicable
billing_reserved_15	If Applicable
agency_agf_percent_rate	Always
contractor_charge_waiver_code	Always
total_line_item_amount	Always
agf_amount	Always
billed_aggregated_tax	Always
line_net_amount	Always

J.2.10.2.1.6 Reserved

J.2.10.2.1.7 Reserved

J.2.10.2.1.8 Direct Billed Agency Setup

Data Transaction Code: DBAS

Note: This data set contains only a single line. If multiple transactions are required, each must be submitted separately.

Element Name	Value Requirement
data_transaction_sequence_num	Always

Element Name	Value Requirement
data_transaction_code	Always
data_transaction_file_date	Always
contract_number	Always
contractor_invoice_level_account_number	Always
agency_task_order_num	Always
agency_identifier	Always
tax_exempt	Always

J.2.10.2.1.9 Dispute

Data Transaction Code: D

Element Name	Value Requirement
data_transaction_sequence_num	If Applicable
data_transaction_code	Always
data_transaction_file_date	Always
contract_number	Always
contractor_service_request_number	Always
contractor_invoice_level_account_number	If Applicable
agency_task_order_num	Always
agency_task_order_modification_number	If Applicable
data_transaction_line_sequence_number	Always
agency_service_request_number_1	If Applicable
agency_service_request_number_2	If Applicable

Element Name	Value Requirement
unique_billing_identifier	If Applicable
agency_hierarchy_code	If Applicable~~Always~~
contract_line_item_number	If Applicable~~Always~~
clin_description	If Applicable~~Always~~
individual_case_basis_code_number	If Applicable
quantity	If Applicable
charging_frequency_and_sre_element_code	If Applicable
charging_unit_code	If Applicable
base_line_item_price	If Applicable
iconectiv_nsc	If Applicable~~Always~~
terminating_iconectiv_nsc	If Applicable
contractor_invoice_number	Always
contractor_invoice_date	If Applicable
billing_period	If Applicable
billing_begin_date	If Applicable
billing_end_date	If Applicable
band_amount	If Applicable
service_connect_start_date_and_time	If Applicable

Element Name	Value Requirement
service_connect_end_date_and_time	If Applicable
billing_authorization_code	If Applicable
originating_number	If Applicable
originating_jurisdiction_code	If Applicable
terminating_jurisdiction_code	If Applicable
usage_event_id	If Applicable
billing_quantity	If Applicable
billing_reserved_01	If Applicable
billing_reserved_02	If Applicable
billing_reserved_03	If Applicable
billing_reserved_04	If Applicable
billing_reserved_05	If Applicable
billing_reserved_06	If Applicable
billing_reserved_07	If Applicable
billing_reserved_08	If Applicable
billing_reserved_09	If Applicable
billing_reserved_10	If Applicable
billing_reserved_11	If Applicable
billing_reserved_12	If Applicable
billing_reserved_13	If Applicable
billing_reserved_14	If Applicable
billing_reserved_15	If Applicable

Element Name	Value Requirement
total_line_item_amount	If Applicable
agf_amount	If Applicable
billed_aggregated_tax	If Applicable
line_net_amount	If Applicable
original_bill_line_item_sequence_number	If Applicable
original_bill_billing_period	If Applicable
disputed_date	If Applicable
dispute_status_code	Always
agency_dispute_number	Always
dispute_reason_code	Always
disputed_charge	If Applicable
disputed_aggregated_tax	If Applicable
disputed_detail_tax_billed	If Applicable
contractor_dispute_adjustment_comments	If Applicable
tax_item_number	If Applicable
agency_comments	If Applicable
contractor_comments	If Applicable

J.2.10.2.1.10 Dispute Report

Data Transaction Code: DR

- Values for unique_billing_identifier, agency_hierarchy_code, contract_line_item_number, clin_description, and iconectiv_nsc may be omitted on data rows associated with the Billing Data Accuracy KPI (see Section G.4.12.1), the Billing Charges Accuracy KPI (see Section G.4.12.2), or the associated Billing Accuracy SLA (see Section G.8.2.3).

Element Name	Value Requirement
data_transaction_code	Always
data_transaction_file_date	Always
contract_number	Always
contractor_service_request_number	If Applicable~~Always~~
contractor_invoice_level_account_number	If Applicable
agency_task_order_num	Always
agency_task_order_modification_number	If Applicable
data_transaction_line_sequence_number	Always
agency_service_request_number_1	If Applicable
agency_service_request_number_2	If Applicable
unique_billing_identifier	Always
agency_hierarchy_code	Always
contract_line_item_number	Always
clin_description	Always
individual_case_basis_code_number	If Applicable
quantity	If Applicable
fully_loaded_price_code	If Applicable
charging_frequency_and_sre_element_code	If Applicable
charging_unit_code	If Applicable
base_line_item_price	If Applicable
iconectiv_nsc	Always
terminating_iconectiv_nsc	If Applicable
contractor_invoice_number	If Applicable

Element Name	Value Requirement
contractor_invoice_date	If Applicable
billing_period	If Applicable
billing_begin_date	If Applicable
billing_end_date	If Applicable
band_amount	If Applicable
service_connect_start_date_and_time	If Applicable
service_connect_end_date_and_time	If Applicable
billing_authorization_code	If Applicable
originating_number	If Applicable
originating_jurisdiction_code	If Applicable
terminating_jurisdiction_code	If Applicable
usage_event_id	If Applicable
billing_quantity	If Applicable
billing_reserved_01	If Applicable
billing_reserved_02	If Applicable
billing_reserved_03	If Applicable
billing_reserved_04	If Applicable
billing_reserved_05	If Applicable
billing_reserved_06	If Applicable
billing_reserved_07	If Applicable
billing_reserved_08	If Applicable
billing_reserved_09	If Applicable
billing_reserved_10	If Applicable

Element Name	Value Requirement
billing_reserved_11	If Applicable
billing_reserved_12	If Applicable
billing_reserved_13	If Applicable
billing_reserved_14	If Applicable
billing_reserved_15	If Applicable
total_line_item_amount	If Applicable
agf_amount	If Applicable
billed_aggregated_tax	If Applicable
line_net_amount	If Applicable
original_bill_line_item_sequence_number	If Applicable
original_bill_billing_period	If Applicable
disputed_date	Always
dispute_status_code	Always
agency_dispute_number	Always
contractor_dispute_number	Always
dispute_reason_code	Always
disputed_charge	If Applicable
disputed_aggregated_tax	If Applicable
disputed_detail_tax_billed	If Applicable
adjustment_date	If Applicable
adjustment_amount	If Applicable
adjustment_aggregated_tax	If Applicable
adjustment_detail_tax_billed	If Applicable

Element Name	Value Requirement
adjustment_reason	Always
adjustment_outcome	Always
contractor_dispute_adjustment_comments	If Applicable
tax_item_number	If Applicable
agency_comments	If Applicable
contractor_comments	If Applicable

J.2.10.2.1.11 Firm Order Commitment Notice

Data Transaction Code: FOCN

Element Name	Unique Value Level	Value Requirement
data_transaction_sequence_num	Data Set	Always
data_transaction_code	Data Set	Always
data_transaction_file_date	Data Set	Always
contract_number	Data Set	Always
order_header_type_code	Data Set	Always
contractor_service_request_number	Data Set	Always
contractor_invoice_level_account_number	Data Set	Always
contractor_service_level_account_number	Data Set	If Applicable
agency_task_order_num	Data Set	Always
agency_task_order_modification_number	Data Set	If Applicable
contractor_price_quote_identifier	Data Set	If Applicable
firm_order_commitment_date	Data Set	If Applicable

Element Name	Unique Value Level	Value Requirement
agency_service_request_number_1	Line Item	If Applicable
agency_service_request_number_2	Line Item	If Applicable
contractor_comments	Data Set	If Applicable

J.2.10.2.1.12 Inventory Reconciliation

Data Transaction Code: IR

Element Name	Value Requirement
data_transaction_code	Always
contract_number	Always
contractor_invoice_level_account_number	Always
contractor_service_level_account_number	Always
agency_task_order_num	Always
data_transaction_line_sequence_number	Always
agency_service_request_number_1	If Applicable
agency_service_request_number_2	If Applicable
unique_billing_identifier	Always
agency_hierarchy_code	Always
iconectiv_nsc	Always
terminating_iconectiv_nsc	If Applicable
building	If Applicable
floor	If Applicable
room	If Applicable

Element Name	Value Requirement
access_provisioning_code	If Applicable
access_circuit_type_code	If Applicable
bandwidth_code	If Applicable
telecommunication_service_priority	If Applicable
local_exchange_carrier_circuit_number	If Applicable
access_diversity	If Applicable
private_virtual_circuit_num	If Applicable
contractor_switch	If Applicable
contractor_trunk	If Applicable
billing_telephone_number	If Applicable
contractor_transport_circuit_number	If Applicable
manufacturer	If Applicable
model	If Applicable
serial_number	If Applicable
phone_number_toll_free_and_700_number	If Applicable
card_number	If Applicable
alternate_code_description	If Applicable
directed_to_number	If Applicable
presubscribed_interexchange_carrier	If Applicable
body_detail_reserved_01	If Applicable
body_detail_reserved_02	If Applicable
body_detail_reserved_03	If Applicable

Element Name	Value Requirement
body_detail_reserved_04	If Applicable
body_detail_reserved_05	If Applicable
body_detail_reserved_06	If Applicable
body_detail_reserved_07	If Applicable
body_detail_reserved_08	If Applicable
body_detail_reserved_09	If Applicable
body_detail_reserved_10	If Applicable
body_detail_reserved_11	If Applicable
body_detail_reserved_12	If Applicable
body_detail_reserved_13	If Applicable
body_detail_reserved_14	If Applicable
body_detail_reserved_15	If Applicable

J.2.10.2.1.13 Monthly Billing Information Memorandum

Data Transaction Code: Not Applicable

Unless otherwise specified by the TO, the contractor may use its standard commercial report format for this report provided it contains sufficient data to:

- Uniquely identify the associated BI
- Clearly communicate key elements in the BI that require explanation or background information
- Provide an overview of the contractor's reasoning, explanation and/or background information

J.2.10.2.1.14 Service Level Agreement Report

Data Transaction Code: SLAR

- Although specified as “If Applicable”, values are always required for “unique_billing_identifier”, “agency_hierarchy_code”, and “service” except for the

Billing Data Accuracy KPI (see Section G.4.12.1) and the Billing Charges Accuracy KPI (see Section G.4.12.2).

- For KPIs measured and reported at the level of the service (see Section G.8.2.1.1), the “unique_billing_identifier” shall contain the value of the primary service component rather than reporting each component separately.

Element Name	Value Requirement
data_transaction_code	Always
data_transaction_file_date	Always
contract_number	Always
agency_task_order_num	Always
data_transaction_line_sequence_number	Always
unique_billing_identifier	If Applicable
agency_hierarchy_code	If Applicable~~Always~~
billing_period	Always
service	If Applicable
sla_performance_period	Always
key_performance_indicator_unit_type_code	Always
key_performance_indicator_measurement	Always
key_performance_indicator_result	Always
service_outage_trouble_ticket_number	If Applicable
service_outage_net_time_to_restore	If Applicable
service_outage_occurred_date_&_time	If Applicable
service_outage_cleared_date_&_time	If Applicable
sla_item_identification	Always

J.2.10.2.1.15 Service Order

Data Transaction Code: SO

When submitted via any means other than the contractor's web interface, the government may use a variety of structured or unstructured formats for this data set unless otherwise specified by the TO. In all cases, the data set submitted by the government will contain sufficient information for the contractor to successfully complete the order and meet contract and TO requirements. The information that the contractor shall collect includes but is not limited to:

- TO Number and TO Modification Number (if applicable)
- Header Level Order Type
- Customer Want Date and Early Installation Approval/Disapproval
- Contact information for COR
- Government project code (optional)
- Line Item Details:
  - Line Item Level Order Type
    - If type is Administrative, see Section J.2.10.2.1.1 Administrative Change Order
  - AHC
  - ASRN(s)
  - CLIN
  - Quantity
- Any comments from the government on handling the order
- Any data elements necessary to successfully complete the order or required by the TO
- If the header level order type is Supplement (see also Section J.2.10.1.1.4.3), the government will include sufficient information to clearly communicate:
  - The order being updated (e.g. CSRN)
  - The line items being updated
  - Updates to be made

When submitted via the contractor's web interface, the government will use the format required by that interface for this data set and will supply the data elements marked as required on that interface.

Note: The contractor shall be responsible for collecting all order information from the government necessary to complete all other deliverables. The contractor may, with OCO concurrence, further define how that data is provided - e.g. limiting the number of

different AHCs or ASRNs that may be processed on a single order, requiring pre-registration of project codes, etc.

J.2.10.2.1.16 Service Order Acknowledgement

Data Transaction Code: SOA

Element Name	Unique Value Level	Value Requirement
data_transaction_sequence_num	Data Set	Always
data_transaction_code	Data Set	Always
data_transaction_file_date	Data Set	Always
contract_number	Data Set	Always
order_header_type_code	Data Set	Always
contractor_service_request_number	Data Set	Always
contractor_invoice_level_account_number	Data Set	Always
agency_task_order_num	Data Set	Always
agency_task_order_modification_number	Data Set	If Applicable
agency_order_sent_date	Data Set	Always
agency_service_request_number_1	Line Item	If Applicable
agency_service_request_number_2	Line Item	If Applicable

J.2.10.2.1.17 Service Order Administrative Change

Data Transaction Code: SOAC

Either/Or value requirement:

- contractor_service_request_number: Populate only if the data element being changed has a Unique Value Level of “Data Set” on the original SOCN (i.e., it is an order value).
- unique_billing_identifier: Populate only if the data element being changed has a Unique Value Level of “Line Item” on the original SOCN (i.e., it is an order line item value).

Element Name	Unique Value Level	Value Requirement
data_transaction_sequence_num	Data Set	Always
data_transaction_code	Data Set	Always
data_transaction_file_date	Data Set	Always
contract_number	Data Set	Always
contractor_service_request_number	Data Set	Either/Or
unique_billing_identifier	Line Item	Either/Or
change_type	Line Item	Always
change_field	Line Item	Always
change_value_from	Line Item	Always
change_value_to	Line Item	Always

J.2.10.2.1.18 Service Order Completion Notice

Data Transaction Code: SOCN

Either/Or value requirement:

- location_state: Populate only if the location is within a jurisdiction with a valid state value.
- location_province: Populate only if the location is within a jurisdiction with a valid ~~state~~ province value.
- If the location is in a country/jurisdiction with no legally recognized states or provinces, both location_state and location_province may be left blank.

Element Name	Unique Value Level	Value Requirement
data_transaction_sequence_num	Data Set	Always
data_transaction_code	Data Set	Always
data_transaction_file_date	Data Set	Always

Element Name	Unique Value Level	Value Requirement
contract_number	Data Set	Always
order_method_code	Data Set	Always
order_header_type_code	Data Set	Always
contractor_service_request_number	Data Set	Always
contractor_invoice_level_account_number	Data Set	Always
contractor_service_level_account_number	Data Set	Always
agency_task_order_num	Data Set	Always
agency_task_order_modification_number	Data Set	If Applicable
contractor_price_quote_identifier	Data Set	If Applicable
agency_project_code	Data Set	If Applicable
agency_order_sent_date	Data Set	Always
customer_want_date	Data Set	If Applicable
early_installation_code	Data Set	Always
contracting_officer_representative_email_address	Data Set	Always
order_point_of_contact_email_address	Data Set	If Applicable
order_point_of_contact_first_name	Data Set	If Applicable
order_point_of_contact_last_name	Data Set	If Applicable
order_point_of_contact_work_phone_number	Data Set	If Applicable
order_point_of_contact_work_phone_extension	Data Set	If Applicable
order_point_of_contact_work_mobile_phone_number	Data Set	If Applicable
technical_point_of_contact_email_address	Data Set	If Applicable
technical_point_of_contact_first_name	Data Set	If Applicable

Element Name	Unique Value Level	Value Requirement
technical_point_of_contact_last_name	Data Set	If Applicable
technical_point_of_contact_work_phone_number	Data Set	If Applicable
technical_point_of_contact_work_phone_extension	Data Set	If Applicable
technical_point_of_contact_work_mobile_phone_number	Data Set	If Applicable
firm_order_commitment_date	Data Set	If Applicable
service_order_completion_date	Data Set	Always
agency_service_request_number_1	Line Item	If Applicable
agency_service_request_number_2	Line Item	If Applicable
unique_billing_identifier	Line Item	Always
ubi_state	Line Item	Always
agency_hierarchy_code	Line Item	Always
contract_line_item_number	Line Item	Always
clin_description	Line Item	Always
individual_case_basis_code_number	Line Item	If Applicable
order_item_type_code	Line Item	Always
quantity	Line Item	Always
fully_loaded_price_code	Line Item	Always
charging_frequency_and_sre_element_code	Line Item	Always
charging_unit_code	Line Item	Always
base_line_item_price	Line Item	Always
iconectiv_nsc	Line Item	Always
terminating_iconectiv_nsc	Line Item	If Applicable

Element Name	Unique Value Level	Value Requirement
location_country	Line Item	Always
street_prefix	Line Item	If Applicable
street_number	Line Item	Always
street_name	Line Item	Always
street_type	Line Item	If Applicable
street_suffix	Line Item	If Applicable
location_address_2	Line Item	If Applicable
location_city	Line Item	Always
location_state	Line Item	Either/Or
location_province	Line Item	Either/Or
location_postal_code	Line Item	Always
location_latitude	Line Item	If Applicable
location_longitude	Line Item	If Applicable
building	Line Item	If Applicable
floor	Line Item	If Applicable
room	Line Item	If Applicable
site_poc_email_address	Line Item	If Applicable
site_poc_first_name	Line Item	If Applicable
site_poc_last_name	Line Item	If Applicable
site_poc_work_phone_number	Line Item	If Applicable
site_poc_work_phone_extension	Line Item	If Applicable
site_poc_work_mobile_phone_number	Line Item	If Applicable

Element Name	Unique Value Level	Value Requirement
alt_site_poc_email_address	Line Item	If Applicable
alt_site_poc_first_name	Line Item	If Applicable
alt_site_poc_last_name	Line Item	If Applicable
alt_site_poc_work_phone_number	Line Item	If Applicable
alt_site_poc_work_phone_extension	Line Item	If Applicable
alt_site_poc_work_mobile_phone_number	Line Item	If Applicable
access_provisioning_code	Line Item	If Applicable
access_circuit_type_code	Line Item	If Applicable
bandwidth_code	Line Item	If Applicable
contractor_access_circuit_number	Line Item	If Applicable
contractor_private_line_number	Line Item	If Applicable
telecommunication_service_priority	Line Item	If Applicable
local_exchange_carrier_circuit_number	Line Item	If Applicable
access_diversity	Line Item	If Applicable
access_path_avoidance	Line Item	If Applicable
private_virtual_circuit_num	Line Item	If Applicable
contractor_switch	Line Item	If Applicable
contractor_trunk	Line Item	If Applicable
billing_telephone_number	Line Item	If Applicable
contractor_transport_circuit_number	Line Item	If Applicable
manufacturer	Line Item	If Applicable
model	Line Item	If Applicable

Element Name	Unique Value Level	Value Requirement
upc	Line Item	If Applicable
serial_number	Line Item	If Applicable
access_jack_type_code	Line Item	If Applicable
access_framing_code	Line Item	If Applicable
line_coding_code	Line Item	If Applicable
phone_number_toll_free_and_700_number	Line Item	If Applicable
card_number	Line Item	If Applicable
alternate_code_description	Line Item	If Applicable
directed_to_number	Line Item	If Applicable
presubscribed_interexchange_carrier	Line Item	If Applicable
labor_email_address	Line Item	If Applicable
body_detail_reserved_01	Line Item	If Applicable
body_detail_reserved_02	Line Item	If Applicable
body_detail_reserved_03	Line Item	If Applicable
body_detail_reserved_04	Line Item	If Applicable
body_detail_reserved_05	Line Item	If Applicable
body_detail_reserved_06	Line Item	If Applicable
body_detail_reserved_07	Line Item	If Applicable
body_detail_reserved_08	Line Item	If Applicable
body_detail_reserved_09	Line Item	If Applicable
body_detail_reserved_10	Line Item	If Applicable
body_detail_reserved_11	Line Item	If Applicable

Element Name	Unique Value Level	Value Requirement
body_detail_reserved_12	Line Item	If Applicable
body_detail_reserved_13	Line Item	If Applicable
body_detail_reserved_14	Line Item	If Applicable
body_detail_reserved_15	Line Item	If Applicable
non-recurring_charge_waiver_code	Line Item	Always
originating_jurisdiction_code	Line Item	Always
agency_comments	Data Set	If Applicable
contractor_comments	Data Set	If Applicable
The following data elements are submitted as attachments (see J.2.9.2.2 Attachments via Direct Data Exchange):		
design_documents	Data Set	If Applicable
site_survey_documents	Data Set	If Applicable
circuit_design_document	Data Set	If Applicable
telecommunication_service_priority_documentation	Data Set	If Applicable

J.2.10.2.1.19 Service Order Confirmation

Data Transaction Code: SOC

Element Name	Unique Value Level	Value Requirement
data_transaction_sequence_num	Data Set	Always
data_transaction_code	Data Set	Always
data_transaction_file_date	Data Set	Always
contract_number	Data Set	Always

Element Name	Unique Value Level	Value Requirement
order_header_type_code	Data Set	Always
contractor_service_request_number	Data Set	Always
contractor_invoice_level_account_number	Data Set	Always
agency_task_order_num	Data Set	Always
agency_task_order_modification_number	Data Set	If Applicable
contractor_price_quote_identifier	Data Set	If Applicable
agency_service_request_number_1	Line Item	If Applicable
agency_service_request_number_2	Line Item	If Applicable
contractor_comments	Data Set	If Applicable

J.2.10.2.1.20 Service Order Rejection Notice

Data Transaction Code: SORN

Value Requirement Note: If the order is being rejected due to lack of inclusion of contractor_invoice_level_account_number and/or agency_task_order_num in the order, the contractor may submit the SORN without values in contractor_service_request_number, contractor_invoice_level_account_number, agency_task_order_num. In all other cases, these values are required as specified in the table below.

Element Name	Unique Value Level	Value Requirement
data_transaction_sequence_num	Data Set	Always
data_transaction_code	Data Set	Always
data_transaction_file_date	Data Set	Always
contract_number	Data Set	Always
order_header_type_code	Data Set	Always

Element Name	Unique Value Level	Value Requirement
contractor_service_request_number	Data Set	Always
contractor_invoice_level_account_number	Data Set	Always
agency_task_order_num	Data Set	Always
agency_task_order_modification_number	Data Set	If Applicable
agency_order_sent_date	Data Set	Always
order_rejection_code	Data Set	Always
agency_service_request_number_1	Line Item	If Applicable
agency_service_request_number_2	Line Item	If Applicable
contractor_comments	Data Set	If Applicable

J.2.10.2.1.21 Service State Change Notice

Data Transaction Code: SSCN

Element Name	Unique Value Level	Value Requirement
data_transaction_sequence_num	Data Set	Always
data_transaction_code	Data Set	Always
data_transaction_file_date	Data Set	Always
contract_number	Data Set	Always
unique_billing_identifier	Line Item	Always
ubi_state	Line Item	Always
time_of_state_change	Line Item	Always
contractor_comments	Line Item	If Applicable

J.2.10.2.1.22 SLA Credit Request

Data Transaction Code: SLACR

If the government chooses to manually submit an SLA credit request, it will provide the contractor with a data table in MS Excel or comma-separated value (CSV) format. The data element order listed in the table below will be used in structuring the table – i.e. the column order of the submitted table will match the specified field order. For SLACRs submitted with multiple rows of data, all data elements are included in each row even if unchanged from the previous row.

Element Name	Value Requirement
data_transaction_code	Always
data_transaction_file_date	Always
contract_number	Always
agency_task_order_num	Always
data_transaction_line_sequence_number	Always
unique_billing_identifier	If Applicable
agency_hierarchy_code	If Applicable~~Always~~
billing_period	Always
service	If Applicable
sla_performance_period	Always
key_performance_indicator_unit_type_code	Always
key_performance_indicator_measurement	Always
key_performance_indicator_result	Always
service_outage_trouble_ticket_number	If Applicable
service_outage_net_time_to_restore	If Applicable
service_outage_occurred_date_&_time	If Applicable

Element Name	Value Requirement
service_outage_cleared_date_&_time	If Applicable
sla_item_identification	If Applicable

J.2.10.2.1.23 SLA Credit Request Response

Data Transaction Code: Not Applicable

Unless otherwise specified by the TO, the contractor may use its standard commercial report format for this report provided it contains sufficient data to:

- Uniquely identify the associated SLACR
- Clearly communicate the contractor's agreement or disagreement with the SLACR
- Indicate if the contractor intends to issue a BA
- Provide an overview of the contractor's reasoning in reaching its decision

J.2.10.2.1.24 Tax Detail

Data Transaction Code: TAX

Element Name	Value Requirement
data_transaction_code	Always
data_transaction_file_date	Always
contract_number	Always
data_transaction_line_sequence_number	Always
unique_billing_identifier	Always
iconectiv_nsc	Always
terminating_iconectiv_nsc	If Applicable
contractor_invoice_number	Always
contractor_invoice_date	Always

Element Name	Value Requirement
billing_period	Always
billing_begin_date	Always
billing_end_date	Always
total_line_item_amount	Always
detail_tax_billed	Always
tax_item_number	Always
original_bill_line_item_sequence_number	Always

J.2.10.2.1.25 Trouble Management Incident Performance Report

Data Transaction Code: Not Applicable

Unless otherwise specified by the TO, the contractor may use its standard commercial report format for this report provided it contains the information specified in Section G.8.5.2.4 Trouble Management Incident Performance Report.

J.2.10.2.1.26 Trouble Management Performance Summary Report

Data Transaction Code: Not Applicable

Unless otherwise specified by the TO, the contractor may use its standard commercial report format for this report provided it contains the information specified in Section G.8.5.2.3 Trouble Management Performance Summary Report.

J.2.10.2.2 Data Sets: Reference Data

The tables in this section have a single column, Element Name, which lists the actual element name. This element name is the column heading (first row) in the data file transferred via secure FTP.

Detailed element specifications are provided in Section J.2.10.3 Data Element Specifications. To locate the correct element specification, it is necessary to locate the combination of Data Transaction Code and Element Name.

Note: data sets in this section are transferred from GSA to the contractor and will always include values for all data elements.

J.2.10.2.2.1 Access Circuit Type

Data Transaction Code: CKTTYP

Element Name
code
description
condition

J.2.10.2.2.2 Access Framing

Data Transaction Code: AFRAM

Element Name
code
description
condition

J.2.10.2.2.3 Access Jack Type

Data Transaction Code: JCKTYP

Element Name
code
description
condition

J.2.10.2.2.4 Access Provisioning

Data Transaction Code: APROV

Element Name
code
description

J.2.10.2.2.5 Reserved

J.2.10.2.2.6 Active/Inactive

Data Transaction Code: ACTINA

Element Name
code
description

J.2.10.2.2.7 Adjustment Outcome

Data Transaction Code: ADJOUT

Element Name
code
description

J.2.10.2.2.8 Adjustment Reason

Data Transaction Code: ADJRSN

Element Name
code
description

J.2.10.2.2.9 Agency Bureau Code

Data Transaction Code: ABCODE

Element Name
agency_identifier
agency_description
new_ab_code
sub_bureau_code
active
old_ab_code
agency_name
bureau_name
sub_bureau_name

J.2.10.2.2.10 Allowable Tax

Data Transaction Code: ALLTAX

Element Name
tax_item_number
tax_item_mod_number
description
nsc_state
nsc_county
nsc_city
taxing_authority
service_equipment

Element Name
voice_data
jur_revenue
rate_application_fixed_percent
percent_taxable_of_charge
percent
fixed_rate
max_allowed_by
max_percent
max_fixed_rate
citation
effective_date
end_date

J.2.10.2.2.11 Bandwidth

Data Transaction Code: BANDW

Element Name
code
description

J.2.10.2.2.12 Reserved

J.2.10.2.2.13 Charging Frequency

Data Transaction Code: CRGFRQ

Element Name
code
description

J.2.10.2.2.14 Charging Unit

Data Transaction Code: CRGUNT

Element Name
code
description

J.2.10.2.2.15 Country

Data Transaction Code: CNTRY

Element Name
iso_alpha_2
iso_alpha_3
iso_numeric_code
jurisdiction_ID
aow
country
code
sovereign
postal_name
postal_code_format
comments

J.2.10.2.2.16 Data Transaction Type

Data Transaction Code: DTT

Element Name
code
description

J.2.10.2.2.17 Dispute Reason

Data Transaction Code: DRSN

Element Name
code
description

J.2.10.2.2.18 Dispute Status

Data Transaction Code: DSTUS

Element Name
code
description

J.2.10.2.2.19 KPI AQL Operator

Data Transaction Code: KPIAO

Element Name
code
description

J.2.10.2.2.20 KPI Location Qualifier

Data Transaction Code: KPILQ

Element Name
code
description

J.2.10.2.2.21 KPI Measurement Unit

Data Transaction Code: KPIMU

Element Name
code
description

J.2.10.2.2.22 KPI Service Level Qualifier

Data Transaction Code: KPISLQ

Element Name
code
description

J.2.10.2.2.23 KPI Unit Code

Data Transaction Code: KPIUC

Element Name
code
description

J.2.10.2.2.24 Line Coding

Data Transaction Code: LNECD

Element Name
code
description
condition

J.2.10.2.2.25 LOA Dependencies

Data Transaction Code: LOADEP

Element Name
code
description

J.2.10.2.2.26 Order Rejection

Data Transaction Code: ORDREJ

Element Name
code
description

J.2.10.2.2.27 Order Type: Header Level

Data Transaction Code: ORDHDR

Element Name
code

Element Name
description

J.2.10.2.2.28 Order Type: Line Item Level

Data Transaction Code: ORDITM

Element Name
code
description

J.2.10.2.2.29 Reserved

J.2.10.2.2.30 Service

Data Transaction Code: SVC

Element Name
service_area
service
mandatory_optional
service_code
service_clin_prefix
section_c_reference
section_b_reference
cbsa_based_service

J.2.10.2.2.31 True/False

Data Transaction Code: TRUFLS

Element Name
code
description

J.2.10.2.2.32 Yes/No

Data Transaction Code: YESNO

Element Name
code
description

J.2.10.2.3 Data Sets: Task Order Data

The data sets in this section are submitted to GSA Systems as described in Section J.2.9 Data Transfer Mechanism. The data elements are not defined further in any other section.

Each column is defined below:

- Element Name:
  - The actual element name; it drives the header row for tabular data (e.g. CSV)
- Element Description:
  - A brief description of the element provided
  - May contain a reference to a list of acceptable values

Note:

- All data elements must be present even if empty for the data sets in this section. Valid values are always required for all elements with the following exceptions, which are only required if applicable:
  - task_order_modification_number
  - stop_date
- Data sets in this section do not have a Data Transaction Code

J.2.10.2.3.1 TO CLINs Awarded

The TO CLINs Awarded deliverable is required when not all CLINs for a service have been awarded to the contractor. It contains only the CLINs that were awarded to the contractor within the TO. This data shall be submitted in CSV format via GSA Systems and contain the data elements in the table below.

Element Name	Element Description
contract_number	EIS contract number issued by GSA
task_order_number	TO number issued by the OCO
task_order_modification_number	TO modification number issued by the OCO if applicable
contractor_invoice_level_account_number	The contractor's invoice account number associated with this TO. Note: Each agency may have more than one account. See also J.2.2.4 Task Order Data Management
clin	Individual CLIN as described in Section B.2 Pricing Tables

J.2.10.2.3.2 TO Customer Requirements Document Set

The TO Customer Requirements Document Set deliverable fully describes the TO requirements. The contractor shall submit the following documents in their original formats to GSA Systems:

- Final version of the Request for Proposal (RFP), Request for Quote (RFQ), or equivalent document issued by the agency, inclusive of all amendments
- Any other documents the customer uses to support its requirements
- Final TO Proposal Volumes
- TO Award Document

J.2.10.2.3.3 TO Financials

The TO Financials deliverable contains the financial data for each performance period covered by the TO (i.e. the TO “base” and any TO “option periods”). The table shall include a separate line for each performance period covered by the TO. This data shall be submitted in CSV format to GSA Systems and contain the data elements in the table below.

Element Name	Element Description
contract_number	EIS contract number issued by GSA

Element Name	Element Description
task_order_number	TO number issued by the OCO
task_order_modification_number	TO modification number issued by the OCO if applicable
contractor_invoice_level_account_number	The contractor's invoice account number associated with this TO. Note: Each agency may have more than one account. See also J.2.2.4 Task Order Data Management
to_ceiling	Dollar value ceiling for the TO
performance_begin_date	Performance period begin date
performance_end_date	Performance period end date
performance_period_funding	Dollar value of the funding for the performance period defined by the performance_begin_date and performance_end_date
to_agf_rate	The AGF rate
proration_type	The type of proration to be used on the TO. Valid values are "Month-Length" and "Normalized" (see also Section J.2.5.1.5.1)

J.2.10.2.3.4 TO Country/Jurisdictions Awarded by Service

The TO Country/Jurisdictions Awarded by Service deliverable contains all countries/jurisdictions awarded by service to the contractor within the TO. This data shall be submitted in CSV format to GSA Systems and contain the data elements in the table below.

Element Name	Element Description
contract_number	EIS contract number issued by GSA
task_order_number	TO number issued by the OCO
task_order_modification_number	TO modification number issued by the OCO if applicable
contractor_invoice_level_account_number	The contractor's invoice account number associated with this TO. Note: Each agency may have more than one account. See also J.2.2.4 Task Order Data Management
service_id–	Service ID code defined in the Service data set (see J.2.10.2.2 Data Sets: Reference Data)

Element Name	Element Description
country~~-~~_jurisdiction_id	Country/Jurisdiction ID code as defined in Section B.2 Pricing Tables

J.2.10.2.3.5 TO Key Performance Indicators

The TO Key Performance Indicators deliverable contains all KPIs specific to the TO where: 1) the KPIs are not in the contract, or 2) the TO overrides the contract KPI. This data shall be submitted in CSV format to GSA Systems and contain the data elements in the table below.

Element Name	Element Description
contract_number	EIS contract number issued by GSA
task_order_number	TO number issued by the OCO
task_order_modification_number	TO modification number issued by the OCO if applicable
contractor_invoice_level_account_number	The contractor's invoice account number associated with this TO. Note: Each agency may have more than one account. See also J.2.2.4 Task Order Data Management
service_id	Service ID code defined in the Service data set (see J.2.10.2.2 Data Sets: Reference Data)
~~Clin~~clin	Individual CLIN as described in Section B.2 Pricing Tables
~~lcb~~icb_number	Individual Case Basis number as described in Section B.2 Pricing Tables
kpi_unit_code	KPI code for this line item from the KPI Unit Code data set (see J.2.10.2.2 Data Sets: Reference Data)
location_qualifier	Location qualifier for this line item from the KPI Location Qualifier data set (see J.2.10.2.2 Data Sets: Reference Data)
measurement_unit	Unit of measurement the value is reported in for this line item from the KPI Measurement Unit data set (see J.2.10.2.2 Data Sets: Reference Data)
service_level_qualifier	Service level qualifier for this line item from the KPI Service Level Qualifier data set (see J.2.10.2.2 Data Sets: Reference Data)

Element Name	Element Description
performance_standard	Numeric value of contractual performance standard (e.g. 99.999)
aql_operator	Acceptable Quality Level (AQL) operator that describes the AQL in relation to the performance standard for this line item from the KPI AQL Operator data set (see J.2.10.2.2 Data Sets: Reference Data)

J.2.10.2.3.6 TO Locations Awarded by Service

The TO Locations Awarded by Service deliverable contains customer locations by service awarded to the contractor within the TO for those services not awarded at the country/jurisdiction level. Services awarded at the country/jurisdiction level shall be omitted from this deliverable. This data shall be submitted in CSV format via GSA Systems and contain the data elements in the table below.

Element Name	Element Description
contract_number	EIS contract number issued by GSA
task_order_number	TO number issued by the OCO
task_order_modification_number	TO modification number issued by the OCO if applicable
contractor_invoice_level_account_number	The contractor's invoice account number associated with this TO. Note: Each agency may have more than one account. See also J.2.2.4 Task Order Data Management
service_id	Service ID code defined in the Service data set (see J.2.10.2.2 Data Sets: Reference Data)
location_nsc	Network Site Code for the location as defined in Section J.2.10.1.1.3

J.2.10.2.3.7 TO Officials

The TO Officials deliverable contains all OCOs and CORs (if applicable) associated with the TO. This data shall be submitted in CSV format via GSA Systems and contain the data elements in the table below.

Element Name	Element Description
contract_number	EIS contract number issued by GSA
task_order_number	TO number issued by the OCO

Element Name	Element Description
task_order_modification_number	TO modification number issued by the OCO
contractor_invoice_level_account_number	The contractor's invoice account number associated with this TO. Note: Each agency may have more than one account. See also J.2.2.4 Task Order Data Management
agency_identifier	Agency identification code available from GSA; also included on the Agency Bureau Code reference table
last_name	Official's last name
first_name	Official's first name
work_email_address	Official's work email address
work_office_phone_number	Official's work phone number
work_mobile_phone_number	Official's work mobile phone number
role	Official's role (either OCO or COR)
start_date	Date of TO award or subsequent modification adding the official
stop_date	Date of TO modification removing the official

J.2.10.2.3.8 TO Services Awarded

The TO Services Awarded deliverable contains all services awarded to the contractor within the TO. This data shall be submitted in CSV format via GSA Systems and contain the data elements in the table below.

Element Name	Element Description
contract_number	EIS contract number issued by GSA
task_order_number	TO number issued by the OCO
task_order_modification_number	TO modification number issued by the OCO if applicable
contractor_invoice_level_account_number	The contractor's invoice account number associated with this TO. Note: Each agency may have more than one account. See also J.2.2.4 Task Order Data Management
service_id	Service ID code defined in Section B.1

Element Name	Element Description
all_clins	Were all CLINs associated with the service awarded? • Y = Yes, all CLINs awarded • N = No, not all CLINs awarded (specific CLINs captured on TO CLINs Awarded List)

J.2.10.3 Data Element Specifications

The tables below fully define and specify each data element contained in the data sets to be exchanged as part of the processes described throughout this CDIP.

The following two subsections address different groups of data sets:

- Section J.2.10.3.1.2 Primary Data Element Dictionary contains all primary data elements (see Section J.2.10.2.1 Data Sets: Primary Data)
- Section J.2.10.3.2 Reference Data Element Dictionary contains all reference data elements (see Section J.2.10.2.2 Data Sets: Reference Data)

J.2.10.3.1 Primary Data Element Dictionary

J.2.10.3.1.1 Interpreting the Primary Data Element List

The columns in the Primary Data Element List are defined below.

- Element Name: The actual element name
- Description: A brief description of the element
- Data Type: Specifies the type of data that can be stored in the field. Valid values are:
  - Alpha: Characters in the standard English alphabet (A-Z and a-z) excluding numbers and special characters (punctuation, symbols, etc.) unless required as part of the edit mask or element specifications in Section J.2.10.1.1
  - Alphanumeric: Characters on the standard 104-key US qwerty keyboard excluding the pipe, '|', character
  - BLOB: Binary Large Object (see also Section J.2.9)
  - Numeric: Numbers (0-9) and at most one decimal point '.'; Negative values are preceded by a minus sign, '-'; Percentages are always converted to standard decimal values, e.g., 5% is presented as '0.05'
  - Date: Full date value including 4-digit year, 2-digit month, and 2-digit day (e.g., 2015-01-01)
  - Time: Full time value based on 24-hour clock including 2-digit hour, 2-digit minute, 2-digit second and offset from UTC in hours and minutes (e.g., 13:05:30-04:00)
  - Date/Time: Full date and time value joining the date and time (as described above) separated by an upper case 'T' (e.g., 2015-01-01T13:05:30-04:00)
- Length: Specifies the length (number of characters) allowed in the element
- Edit Mask: Provides internal structure reference for elements with specific structure:
  - Values are superseded by any element specifications in Section J.2.10.1.1
  - The table below defines the values in this column:

Edit Mask Value	Description
Blank Field	Any combination of characters allowed by the data type excluding the pipe character, "|"
A	Any single character in the standard English alphabet (A-Z and a-z; no numbers or special characters); multiple instances indicate the number of consecutive characters (e.g., “AAA” indicates 3 characters)
YYYY-MM-DD	Full date including 4-digit year (YYYY), 2-digit month (MM), and 2-digit day (DD) Example: 2015-01-01
HH:MM:SS+/-hh:mm	Full time based on 24-hour clock including 2-digit hour (HH), 2-digit minute (MM), 2-digit second (SS) and offset (+ or -) from Coordinated Universal Time (UTC) in hours (hh) and minutes (mm) Example: 13:05:30-04:00
HHH:MM:SS	Duration including up to 3 digits for hours (HHH), 2-digit minutes (MM), 2-digit seconds (SS)
N	Any single-digit number (0-9); multiple instances indicate the number of consecutive digits (e.g., “NNN” indicates 3 digits) Note: If an edit mask shows a specific number of decimal places (i.e., digits after the decimal point), the contractor shall not round to fewer decimal places. See also Section J.2.5.1.6 Rounding
Ref: TTTTTT.EEEEEE	The only valid values for this field are defined in a reference table (see Section J.2.10.2.2 Data Sets: Reference Data). The specific reference table and data element within the table are identified using the information after the “Ref:” prefix: TTTTTT (before the “.”) = Data Transaction Code for the table EEEEEE (after the “.”) = Element name within the table When specified, the contractor shall only use values included in the reference table and element combination when populating the data element.
All Other Values	All other values are literal (for example, if the mask includes a comma, ",", a comma is required in that specific position within the value).

J.2.10.3.1.2 Primary Data Element List

Element Name	Description	Data Type	Length	Edit Mask
access_circuit_type_code	Access Circuit Type Code	Alphanumeric	6	Ref: CKTTYP.code
access_diversity	True if circuit assigned diverse access. False otherwise.	Alphanumeric	1	Ref: TRUFLS.code
access_framing_code	Access Framing Code	Alphanumeric	25	Ref: AFRAM.code
access_jack_type_code	Access Jack Type Code	Alphanumeric	25	Ref: JCKTYP.code
access_path_avoidance	True if certain access paths are to be avoided. False otherwise.	Alphanumeric	1	Ref: TRUFLS.code
access_provisioning_code	Code indicating if the access was provided by the contractor or the agency	Alphanumeric	1	Ref: APROV.code
adjustment_aggregated_tax	This is the total adjustments to all taxes, fees, and surcharges including the AGF. This value may omit the AGF at the contractor's discretion provided they provide notice of their choice to their GSA CO and COR and the OCO and COR(s) associated with any awarded TOs. A minus sign indicates the charge is being reduced (i.e., a credit to the agency). If the charge is increased (i.e., a debit to the agency), no indicator is required.~~Adjustment to aggregated tax~~	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN

Element Name	Description	Data Type	Length	Edit Mask
adjustment_amount	This is the total line item amount of the adjustment including individual adjustments to CLIN price, AGF collected, taxes, fees and surcharges. A minus sign indicates the charge is being reduced (i.e., a credit to the agency). If the charge is increased (i.e., a debit to the agency), no indicator is required. ~~Amount of adjustment~~	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN
adjustment_date	Date of adjustment	Date	10	YYYY-MM-DD
adjustment_detail_tax_billed	There are two allowed methods for supplying this data. Method 1: Provide a single line item which is the total adjustments to all taxes, fees, and surcharges normally reported in the TAX detail deliverable. This excludes the AGF. Under this method, tax_item_number is left blank unless otherwise specified in the Task Order (TO). Method 2: Provide individual line items for each adjusted tax, fee, or surcharge normally reported in the TAX detail deliverable. This excludes the AGF. Under this method, tax_item_number is populated with the appropriate value from the Allowable Taxes (ALLTAX) reference table. A minus sign indicates the charge is being reduced (i.e., a credit to the agency). If the charge is increased (i.e., a debit to the agency), no indicator is required.~~Adjustment detail of the aggregated tax~~	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN
adjustment_outcome	Contractor adjustment outcome	Alphanumeric	25~~5~~	Ref: ADJOUT.code
adjustment_reason	Contractor adjustment reason	Alphanumeric	25~~5~~	Ref: ADJRSN.code

Element Name	Description	Data Type	Length	Edit Mask
agency_agf_percent_rate	Agency Associated Government Fee Percent (AGF) rate	Numeric	10	NNN.NNNNNN
agency_comments	Agency comments for describing need and special instructions to Contractor	Alphanumeric	2000	
agency_dispute_number	Agency Dispute Number	Alphanumeric	20	
agency_hierarchy_code	An internal government accounting code and must be tracked for all services from order submission through disconnection	Alphanumeric	28	
agency_identifier	Agency bureau code identifies the agency / sub-agency	Alphanumeric	8	Ref: ABCODE.agency_Identifier
agency_order_sent_date	Date that order was sent by Agency	Date	10	YYYY-MM-DD
agency_project_code	An optional internal government project number	Alphanumeric	50	
agency_service_request_number_1	An optional internal government control number	Alphanumeric	50	
agency_service_request_number_2	An optional internal government control number	Alphanumeric	50	
agency_task_order_modification_number	Agency task order modification number.	Alphanumeric	25	
agency_task_order_num	Agency task order number. Also known as the Procurement Instrument Identifier (PIID)	Alphanumeric	51	
agf_amount	(Total_Line_Item_Amount*Agency_AGF_Percent_Rate)	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN
agf_electronic_funds_transfer_amount	Associated Government Fee (AGF) amount that was wire transferred to GSA	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN

Element Name	Description	Data Type	Length	Edit Mask
agf_electronic_funds_transfer_date	Date that Associated Government Fee (AGF) was wire transferred to GSA	Date	10	YYYY-MM-DD
alt_site_poc_email_address	Originating site alternate Point of Contact (POC) email address	Alphanumeric	100	
alt_site_poc_first_name	Originating site alternate Point of Contact (POC) first name	Alphanumeric	30	
alt_site_poc_last_name	Originating site alternate Point of Contact (POC) last name	Alphanumeric	30	
alt_site_poc_work_mobile_phone_number	Originating site alternate Point of Contact (POC) work mobile phone number	Numeric	15	
alt_site_poc_work_phone_extension	Originating site alternate Point of Contact (POC) work phone number extension	Numeric	5	NNNNN
alt_site_poc_work_phone_number	Originating site alternate Point of Contact (POC) work phone number	Numeric	15	
alternate_code_description	Used for a description when needed (e.g., a name on a calling card or conference bridge)	Alphanumeric	30	
band_amount	Band amount is used to determine a price from a band table. This is not a price amount. This is the usage amount that falls within a band range. For example, if the band is 5-10Mb, and actual usage was 7Mb the value for this element is 7.	Numeric	50	
bandwidth_code	Code that identifies the bandwidth unit of measurement (e.g., 10 Gbps)	Alphanumeric	25	Ref: BANDW.code

Element Name	Description	Data Type	Length	Edit Mask
base_line_item_price	Base price amount of the line item without the AGF	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN
billed_aggregated_tax	Aggregated eligible taxes, fees and surcharges as defined in the allowable tax reference table.	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN
billing_authorization_code	Phone number / calling card number / voice circuit authorization code / toll number used to authorize service	Alphanumeric	20	
billing_begin_date	Effective date service begins for the billed period. This would be the date of new service if service was installed for the billed period. Otherwise this is the first day of the month.	Date	10	YYYY-MM-DD
billing_end_date	Effective date service ends for the billed period. This would be the date of discontinued service if service was disconnected within the billed period. Otherwise this is the last day of the month.	Date	10	YYYY-MM-DD
billing_period	Start date of Invoice billing period; for example invoice for June 2014 would be 2014-06-01 (06/01/2014)	Date	10	YYYY-MM-DD
billing_quantity	This is the quantity that will drive billing changes based on CLIN – i.e., Base_Line_Item_Price multiplied by Billing_Quantity = Total_Line_Item_Price	Numeric	20	NNNNNNNNNNNNNNNN.NN
billing_reserved_01	Reserved for future billing use	Alphanumeric	250	
billing_reserved_02	Reserved for future billing use	Alphanumeric	250	
billing_reserved_03	Reserved for future billing use	Alphanumeric	250	

Element Name	Description	Data Type	Length	Edit Mask
billing_reserved_04	Reserved for future billing use	Alphanumeric	250	
billing_reserved_05	Reserved for future billing use	Alphanumeric	250	
billing_reserved_06	Reserved for future billing use	Alphanumeric	250	
billing_reserved_07	Reserved for future billing use	Alphanumeric	250	
billing_reserved_08	Reserved for future billing use	Alphanumeric	250	
billing_reserved_09	Reserved for future billing use	Alphanumeric	250	
billing_reserved_10	Reserved for future billing use	Alphanumeric	250	
billing_reserved_11	Reserved for future billing use	Alphanumeric	250	
billing_reserved_12	Reserved for future billing use	Alphanumeric	250	
billing_reserved_13	Reserved for future billing use	Alphanumeric	250	
billing_reserved_14	Reserved for future billing use	Alphanumeric	250	
billing_reserved_15	Reserved for future billing use	Alphanumeric	250	
billing_telephone_number	Billing telephone number (BTN) / Circuit Authorization code to allow Voice traffic. Used for trunk billing vs station level billing	Alphanumeric	20	
body_detail_reserved_01	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_02	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_03	Reserved for future Use	Alphanumeric	250	

Element Name	Description	Data Type	Length	Edit Mask
body_detail_reserved_04	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_05	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_06	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_07	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_08	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_09	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_10	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_11	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_12	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_13	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_14	Reserved for future Use	Alphanumeric	250	
body_detail_reserved_15	Reserved for future Use	Alphanumeric	250	
building	Building (Service Delivery Address)	Alphanumeric	20	
card_number	Calling card authorization number	Alphanumeric	20	
change_field	The name of the field to be changed	Alphanumeric	100	

Element Name	Description	Data Type	Length	Edit Mask
change_type	Indicates the Unique Value Level of the data element to be changed as it appears in the SOCN definition. If the data element being changed has a Unique Value Level of “Data Set” on the original SOCN the change type is Order (record as "O"). If the data element being changed has a Unique Value Level of “Line Item” on the original SOCN the change type is Line Item (record as "L"). Expected Values: O = Order L = Line Item	Alpha	1	
change_value_from	The old value that is being changed	Alphanumeric	2000	
change_value_to	The new value being entered	Alphanumeric	2000	
charging_frequency_and_sre_element_code	Charge frequency description (e.g., Monthly Recurring Charge [MRC], Non-Recurring Charge [NRC], Usage, and SRE Pricing Element etc.) Code	Alphanumeric	10	Ref: CRGFRQ.code
charging_unit_code	Code defining the specific charge unit (e.g., per port, per time-increment, etc.)	Alphanumeric	~~10~~5	Ref: CRGUNT.code
circuit_design_document	These documents are to assist with provisioning of service; this may include, but not be limited to, network design, architecture, site survey, Interactive Voice Response (IVR) layout, call center, engineering layout, etc.	BLOB		
clin_description	Contract Line Item Numbers (CLINs) Description	Alphanumeric	100	

Element Name	Description	Data Type	Length	Edit Mask
contract_line_item_number	Contract Line Item Numbers (CLINs). Used to uniquely identify services available on the contract. Agency or Contractor may provide CLINs; all CLINs must be approved via an order by the Agency prior to the activity occurring	Alphanumeric	7	
contract_number	EIS contract number assigned to the contractor. (Not the Task Order number.)	Alphanumeric	20	
contracting_officer_representative_email_address	Contracting Officer Representative (COR) email address	Alphanumeric	100	
contractor_access_circuit_number	The circuit ID should be the one most closely associated with the CLIN. e.g. a port CLIN would require a port circuit ID while an access CLIN would require the access circuit ID	Alphanumeric	100	
contractor_charge_waiver_code	Indicates if the contractor has waived the charge at billing. If the charge is being waived, the base_line_item_price may be reported as either its normal value or as zero (0) as agreed between the contractor and the customer or as indicated in the TO.	Alpha	1	Ref: YESNO.code
contractor_comments	Contractor comments to agency	Alphanumeric	2000	
contractor_direct_billed_agf_adjustment	Adjusted amount that Contractor billed for AGF fee and collected for GSA. A minus sign indicates the charge is being reduced (i.e., a credit to the agency). If the charge is increased (i.e., a debit to the agency), no indicator is required.	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN
contractor_direct_billed_agf_collected	Amount that Contractor billed directly to agency for AGF fee and collected for GSA	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN

Element Name	Description	Data Type	Length	Edit Mask
contractor_dispute_adjustment_comments	Contractor comments for describing dispute or Adjustment	Alphanumeric	2000	
contractor_dispute_number	Unique Contractor Dispute Number	Alphanumeric	20	
contractor_invoice_date	Date of Contractor's invoice	Date	10	YYYY-MM-DD
contractor_invoice_level_account_number	Contractor's invoice account number associated with this transaction (not a central invoice number).	Alphanumeric	25	
contractor_invoice_number	Invoice number assigned by Contractor to monthly invoice	Alphanumeric	20	
contractor_price_quote_identifier	Reference number optionally used to communicate to the customer the specific contractor price quote associated with an order.	Alphanumeric	50	
contractor_private_line_number	A number that uniquely identifies the line that connects two access points in a private line service	Alphanumeric	100	
contractor_service_level_account_number	Contractor's service account number used to group all components of a service on an account that contains numbers or calling cards.	Alphanumeric	50	
contractor_service_request_number	Contractor order number.	Alphanumeric	50	
contractor_switch	Contractor switch number	Numeric	5	
contractor_transport_circuit_number	The circuit ID should be the one most closely associated with the CLIN. e.g. a port CLIN would require a port circuit ID while an access CLIN would require the access circuit ID	Alphanumeric	100	
contractor_trunk	Contractor trunk number	Numeric	5	

Element Name	Description	Data Type	Length	Edit Mask
customer_want_date	Customer's requested provisioning date	Date	10	YYYY-MM-DD
data_transaction_code	Identifies the transaction represented by the file or data exchange	Alphanumeric	~~10~~6	Ref: DTT.code
data_transaction_file_date	Submission date for the data set	Date	10	YYYY-MM-DD
data_transaction_line_sequence_number	Data Transaction line sequence number. The contractor shall assign a unique data transaction line sequence number to each record within a deliverable.	Numeric	14	
data_transaction_sequence_num	Uniquely identifies each data exchange transaction. In the event it becomes necessary to examine a transaction in detail, this number will ensure all parties are referring to the same transaction. Other than the data type and length, the submitting party is free to create this number in any manner desired - e.g., a millisecond-level timestamp based on data submission time.	Numeric	20	NNNNNNNNNNNNNNNNNNNN
design_documents	Engineering documents to cover elements that are not covered in order data	BLOB		
detail_tax_billed	Detail of the aggregated eligible taxes, fees and surcharges	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN
directed_to_number	The number the toll-free number is to be directed to	Alphanumeric	13	
dispute_reason_code	Code corresponding to reason for dispute	Alphanumeric	10	Ref: DRSN.code
dispute_status_code	Disputed Status Code from Agency	Alphanumeric	1	Ref: DSTUS.code

Element Name	Description	Data Type	Length	Edit Mask
disputed_aggregated_tax	Amount of the aggregated tax in dispute	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN
disputed_charge	Disputed Charge associated with record identified	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN
disputed_date	Date the Agency opens a dispute	Date	10	YYYY-MM-DD
disputed_detail_tax_billed	Disputed detail of the aggregated tax	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN
early_installation_code	Will Agency accept services prior to contractual due date?	Alpha	1	Ref: YESNO.code
firm_order_commitment_date	Firm date for service installation	Date	10	YYYY-MM-DD
floor	Floor (Service Delivery Address)	Alphanumeric	10	
fully_loaded_price_code	Is the base price fully loaded as defined in the contract?	Alpha	1	Ref: YESNO.code
~~gsa_account_number~~	~~GSA Account Number is account number provided after TO award~~	~~Alphanumeric~~	~~20~~	
iconectiv_nsc	ICONECTIV Network Site Code for the originating location (Service Delivery Address)	Alphanumeric	20	
individual_case_basis_code_number	Individual Case Basis (ICB) number submitted with Contract Line Item Number (CLIN). Agency or Contractor may provide CLINs. All CLINs must be approved via an order by the Agency prior to the activity occurring	Alphanumeric	50	

Element Name	Description	Data Type	Length	Edit Mask
key_performance_indicator_measurement	This is the name of the KPI specified in a manner that is intended to be easily understood by CORs and other agency representatives (e.g., 'Latency in continental US (CONUS)', 'Service Provisioning', etc.)~~Name of the KPI (e.g., Availability)~~	Alphanumeric	60	
key_performance_indicator_result	Contractor's Key Performance Indicator (KPI) results	Numeric	60	
key_performance_indicator_unit_type_code	Key Performance Indicator (KPI) type that describes the KPI category	Alphanumeric	~~20~~6	Ref: KPIUC.code
labor_email_address	Email address of person performing labor services under SRL	Alphanumeric	100	
line_coding_code	Line Coding Code	Alphanumeric	5	Ref: LNECD.code
line_net_amount	(Total_Line_Item_Amount + AGF_Amount + Billed_Aggregated_Tax +	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN
local_exchange_carrier_circuit_number	Local Exchange Carrier (LEC) circuit number	Alphanumeric	100	
location_address_2	Second line of new address for this order location (Service Delivery Address)	Alphanumeric	100	
location_city	City for this order location (Service Delivery Address)	Alphanumeric	60	
location_country	Country for this order location (Service Delivery Address)	Alphanumeric	50	Ref: CNTRY.country
location_latitude	Delivery latitude (Service Delivery Address)	Numeric	13	
location_longitude	Delivery longitude (Service Delivery Address)	Numeric	13	

Element Name	Description	Data Type	Length	Edit Mask
location_postal_code	Postal code for this order location (Service Delivery Address)	Alphanumeric	10	
location_province	Province for this order location (Service Delivery Address)	Alpha	50	
location_state	State for this order location (Service Delivery Address)	Alpha	50	
manufacturer	Manufacturer	Alphanumeric	50	
model	Model (e.g., service related equipment model)	Alphanumeric	50	
non-recurring_charge_waiver_code	Non-Recurring Charge (NRC) waiver Yes or No	Alpha	1	Ref: YESNO.code
order_header_type_code	Indicates the overall order type	Alphanumeric	1	Ref: ORDHDR.code
order_item_type_code	Indicates the order type for this line item	Alphanumeric	1	Ref: ORDITM.code
order_method_code	D = direct. Note: unless otherwise specified in the TO, this value is always D	Alpha	1	
order_point_of_contact_email_address	Order Point of Contact (POC) email address	Alphanumeric	100	
order_point_of_contact_first_name	Order Point of Contact First Name	Alphanumeric	30	
order_point_of_contact_last_name	Order Point of Contact Last Name	Alphanumeric	30	
order_point_of_contact_work_mobile_phone_number	Order Point of Contact Work Mobile Phone Number	Numeric	15	
order_point_of_contact_work_phone_extension	Order Point of Contact Work Phone Extension	Numeric	5	NNNNN

Element Name	Description	Data Type	Length	Edit Mask
order_point_of_contact_work_phone_number	Order Point of Contact Work Phone Number	Numeric	15	
order_rejection_code	Reason for order rejection	Alphanumeric	25	Ref: ORDREJ.code
original_bill_billing_period	First day of Original Bill Billing Period.	Date	10	YYYY-MM-DD
original_bill_line_item_sequence_number	Original Bill Line Item Sequence number.	Numeric	14	
originating_jurisdiction_code	Applies to domestic (CONUS/OCONUS) or non-domestic	Numeric	6	Ref: CNTRY.jurisdiction_ID
originating_location_city	City for this order location, always applies to domestic (CONUS/OCONUS)	Alphanumeric	50	
originating_location_country	Country for this order location	Alpha~~numeric~~	2	Ref: CNTRY.iso_alpha_2
originating_location_county	County for this order location, always applies to domestic (CONUS/OCONUS)	Alphanumeric	50	
originating_location_state	State for this order location, always applies to domestic (CONUS/OCONUS)	Alpha	50	
originating_number	Calling number (number identifier from which a call originates)	Alphanumeric	20	
phone_number_toll_free_and_700_number	Phone number associated with phone number CLINs. e.g. desk phone, cell phones, toll free number, Wi-Fi hotspot, etc.	Alphanumeric	10	

Element Name	Description	Data Type	Length	Edit Mask
presubscribed_interexchange_carrier	Is there a Presubscribed Interexchange Carrier (PIC)? if no, there is no long distance service for this line	Alpha	1	Ref: YESNO.Code
private_virtual_circuit_num	Private Virtual Circuit Number	Alphanumeric	30	
quantity	Numeric count for the item specified by the Contract Line Item Number (CLIN)	Numeric	9	NNNNNNNNN
room	Room (Service Delivery Address)	Alphanumeric	10	
serial_number	Serial number for SRE	Alphanumeric	50	
service	Service	Alphanumeric	20	Ref: SVC.service_code
service_connect_end_date_and_time	Service disconnect date and time or call connection end date and time	Date/time	252	YYYY-MM-DDTHH:MM:SS+/-hh:mm
service_connect_start_date_and_time	Service connect date and time or call connection start date and time	Date/time	252	YYYY-MM-DDTHH:MM:SS+/-hh:mm
service_order_completion_date	Date service was completed	Date	10	YYYY-MM-DD
service_outage_cleared_date_&_time	Service outage cleared date and time	Date/time	252	YYYY-MM-DDTHH:MM:SS+/-hh:mm
service_outage_net_time_to_restore	Service outage Time to Restore	Numeric	9	HHH:MM:SS

Element Name	Description	Data Type	Length	Edit Mask
service_outage_occurred_date_&_time	Service outage occurred date and time	Date/time	252	YYYY-MM-DDTHH:MM:SS+/-hh:mm
service_outage_trouble_ticket_number	Service outage trouble ticket number	Alphanumeric	60	
site_poc_email_address	Service Location Point of Contact (POC) email address	Alphanumeric	100	
site_poc_first_name	Service Location Point of Contact (POC) First Name	Alphanumeric	30	
site_poc_last_name	Service Location Point of Contact (POC) Last Name	Alphanumeric	30	
site_poc_work_mobile_phone_number	Service Location Point of Contact (POC) Mobile phone number of Contact	Numeric	15	
site_poc_work_phone_extension	Service Location Point of Contact (POC) Phone extension of Contact	Numeric	5	NNNNN
site_poc_work_phone_number	Service Location Point of Contact (POC) Phone Number of Contact	Numeric	15	
site_survey_documents	Site survey documents	BLOB		
sla_item_identification	SLA reported Identification. This is used to identify the missed SLA in the SLA credit request and any resulting disputes and/or billing adjustments	Alphanumeric	60	
sla_performance_period	SLA reporting period when service was performed. for example invoice for June 2014 would be 06/01/2014	Date	10	YYYY-MM-DD

Element Name	Description	Data Type	Length	Edit Mask
street_name	The street name of the address (Service Delivery Address)	Alphanumeric	100	
street_number	The street number of the address (Service Delivery Address)	Alphanumeric	15	
street_prefix	The street prefix of the address (e.g., W, N, SE, ...) (Service Delivery Address)	Alphanumeric	10	
street_suffix	The street suffix of the address (e.g., W, N, SE, ...) (Service Delivery Address)	Alphanumeric	10	
street_type	The street type of the address (e.g., AVE, HWY, ...) (Service Delivery Address)	Alphanumeric	25	
tax_exempt	Is the agency or organization exempt from all taxes and surcharges (e.g., World Bank and IMF)?	Alpha	1	Ref: YESNO.code
tax_item_number	Tax Item Number to identify items in the allowable tax table	Alphanumeric	20	Ref: ALLTAX.tax_item_number
technical_point_of_contact_email_address	Technical Point of Contact (POC) email address	Alphanumeric	100	
technical_point_of_contact_first_name	Technical Point of Contact First Name	Alphanumeric	30	
technical_point_of_contact_last_name	Technical Point of Contact Last Name	Alphanumeric	30	
technical_point_of_contact_work_mobile_phone_number	Technical Point of Contact Work Mobile Phone Number	Numeric	15	
technical_point_of_contact_work_phone_extension	Technical Point of Contact Work Phone Extension	Numeric	5	NNNNN

Element Name	Description	Data Type	Length	Edit Mask
technical_point_of_contact_work_phone_number	Technical Point of Contact Work Phone Number	Numeric	15	
telecommunication_service_priority	Telecommunication Service Priority (TSP) code enabling timely Service restoration in adverse events	Alphanumeric	12	AAAAAAAAA-AA
telecommunication_service_priority_documentation	This is the Telecommunication Service Priority (TSP) official attachment for records	BLOB		
terminating_iconectiv_nsc	ICONECTIV Network Site Code for the terminating location (Service Delivery Address)	Alphanumeric	20	
terminating_jurisdiction_code	Jurisdiction Code for the terminating location	Numeric	6	Ref: CNTRY.jurisdiction_ID
terminating_location_city	City for this order location	Alphanumeric	50	
terminating_location_country	Country for this order location	Alpha~~numeric~~	2	Ref: CNTRY.iso_alpha_2
terminating_location_county	County for this order location	Alphanumeric	50	
terminating_location_state	State for this order location	Alpha	50	
terminating_number	Terminating number on which the call finalized (forwarded call)	Alphanumeric	20	
time_of_state_change	Timestamp marking change in service state (e.g., change in auto-sold CLIN state)	Date/time	252	YYYY-MM-DDTHH:MM:SS+/-hh:mm

Element Name	Description	Data Type	Length	Edit Mask
total_line_item_amount	(Base_Line_Item_Price*Billing_Quantity). This is the taxable amount. NO AGF, Taxes, or Surcharges may be in this amount.	Numeric	23	NNNNNNNNNNNNNNNN.NNNNNN
ubi_state	The current service state of the UBI. Options are: Active = The UBI is active with charges accumulating Inactive = The UBI is inactive with no charges accumulating Band_Name = The band-priced UBI is in the band listed. Note: the state is the actual band name/designator as defined in Section B and/or the TO	Alphanumeric	50	
unique_billing_identifier	Uniquely identifies one or more items linked together for ordering, billing and inventory management purposes	Alphanumeric	86	
upc	Universal Product Code (ori) for SRE	Alphanumeric	50	
usage_event_id	This ID is used to group conference call charges etc.	Alphanumeric	20	

J.2.10.3.2 Reference Data Element Dictionary

J.2.10.3.2.1 Interpreting the Reference Data Element List

The columns in the Reference Data Element List are defined below:

- Data Transaction Code: Code for the reference table that contains the element (see Section J.2.10.1.1.5)
- Element Name: The actual element name
- Description: A brief description of the element. May also include:
  - An edit mask (see Section J.2.10.3.1.1)
  - Example or expected values
    - Note: Any values listed are representative only. The government will separately provide definitions of any codes used prior to including them in initial or updated reference tables (see Section J.2.3.2.1).
  - Connections to other reference tables
- Data Type: Specifies the type of data that can be stored in the field. Valid values are:
  - Alpha: Characters in the standard English alphabet (A-Z and a-z) excluding numbers and special characters (punctuation, symbols, etc.) unless required as part of the edit mask or element specifications in Section J.2.10.1.1
  - Alphanumeric: Characters on the standard 104-key US qwerty keyboard excluding the pipe, '|', character
  - Date/time: Full date and time
  - Numeric: Numbers (0-9) and at most one decimal point '.'; Negative values are represented by preceding the number with a minus sign, '-'; Percentages are always converted to standard decimal values, e.g., 5% is presented as '0.05'
- Length: Specifies the length (number of characters) allowed in the element

J.2.10.3.2.2 Reference Data Element Dictionary Table

Data Transaction Code	Element Name	Description	Data Type	Length
ABCODE	active	Status: Active / Inactive; will contain value from reference table Active/Inactive (code field)	Alpha	1
ABCODE	agency_description	GSA Agency Description	Alphanumeric	9
ABCODE	agency_identifier	GSA Agency Identifier	Alphanumeric	8
ABCODE	agency_name	Name of organization to be established as agency	Alphanumeric	100
ABCODE	bureau_name	Name of organization to be established as Bureau	Alphanumeric	100
ABCODE	new_ab_code	Agency Bureau Code	Alphanumeric	5
ABCODE	old_ab_code	Contract short Description assigned by GSA to identify Contractor and contract type. (Contractor + Contract)	Alphanumeric	4
ABCODE	sub_bureau_code	Sub Bureau Code	Alphanumeric	4
ABCODE	sub_bureau_name	Name of organization to be established as Sub Bureau	Alphanumeric	100
ACTINA	code	Active or Inactive Code	Alphanumeric	1
ACTINA	description	Active or Inactive Description	Alphanumeric	256
ADJOUT	code	Adjustment Outcome Code	Alphanumeric	25
ADJOUT	description	Adjustment Outcome Description	Alphanumeric	256
ADJRSN	code	Adjustment Reason Code	Alphanumeric	25

Data Transaction Code	Element Name	Description	Data Type	Length
ADJRSN	description	Adjustment Reason Description	Alphanumeric	256
AFRAM	code	Access Framing Code	Alphanumeric	25
AFRAM	condition	Access Framing Condition	Alphanumeric	50
AFRAM	description	Access Framing Description	Alphanumeric	256
ALLTAX	citation	Taxation authority reference. Indicate by exact legal reference such as Statute, DR Rule, County Code, etc. Example: AZ Statute §42-5064	Alphanumeric	255
ALLTAX	description	A descriptive code for the tax. Expected values: GR = Gross Receipts, B + Business, U = Utility, ST = Sales Tax, FUSF = Federal Universal Service Fund, I = Infrastructure, PUC = Public Utility Commission, FUSA = Federal Hearing Impaired, NP = Number Portability, FRS = Federal Relay Service, STRS = State Telecommunications Relay Service, SUSF = State Universal Service Fund, OTHR = Other, 911 = 911	Alphanumeric	4
ALLTAX	effective_date	Date to begin collection of tax. Edit Mask: YYYY-MM-DDTHH:MM:SS+/-hh:mm	Date/time	252
ALLTAX	end_date	Date tax collection ends. Edit Mask: YYYY-MM-DDTHH:MM:SS+/-hh:mm	Date/time	252
ALLTAX	fixed_rate	Allowable Fixed Rate. Edit Mask: NNNNNNNNNNNNNNN.NNNNNN	Numeric	23

Data Transaction Code	Element Name	Description	Data Type	Length
ALLTAX	jur_revenue	Indicate jurisdiction of the revenues to which the tax is to be applied: (Interstate, Intrastate, or Both). Expected values: A = Intrastate, E = Interstate, B = Both, N = Not Applicable	Alpha	1
ALLTAX	max_allowed_by	State, County, City / County City / State City / County State. Expected values: SCC = State, County, City; CC = County, City; SC = State, City, CS = County, State	Alpha	3
ALLTAX	max_fixed_rate	Max fixed rate allowed. Edit Mask: NNNNNNNNNNNNNNN.NNNNNN	Numeric	23
ALLTAX	max_percent	Max percent allowed. Edit Mask: NNN.NNNNNN	Numeric	10
ALLTAX	nsc_city	City for the Tax	Alpha	100
ALLTAX	nsc_county	County for the Tax	Alpha	100
ALLTAX	nsc_state	State for the Tax	Alpha	2
ALLTAX	percent	Allowable Tax Percent. Edit Mask: NNN.NNNNNN	Numeric	10
ALLTAX	rate_application_fixed_percent	Indicate whether tax is fixed amount, percent or both. Expected values: F = Fixed, P = Percent, B = Both	Alpha	1
ALLTAX	percent_taxable_of_charge	Percent of Charge that is taxable. Edit Mask: NNN.NNNNNN	Numeric	10

Data Transaction Code	Element Name	Description	Data Type	Length
ALLTAX	service_equipment	Tax applies to Services, Equipment or Both (No taxes on labor or travel reimbursement). Expected values: S = Service, E = Equipment, B = Service & Equipment, A = Account, L = Line, O = Other	Alpha	1
ALLTAX	tax_item_mod_number	Tax Item Modification Number	Alphanumeric	20
ALLTAX	tax_item_number	Tax Identification Number	Alphanumeric	20
ALLTAX	taxing_authority	Indicate jurisdiction of the taxing authority: (FED, ST, CO, CI). Expected values: ST = State, CO = County, CI = City, Fed = Federal, SD = School District, O = Other	Alpha	3
ALLTAX	voice_data	Tax applies to Voice, Data, Both. Expected values: V = Voice, D = Data, B = Voice & Data, N = Not Applicable	Alpha	1
APROV	code	Access Provisioning Provider Code	Alphanumeric	1
APROV	description	Access Provisioning Provider Description	Alphanumeric	256
BANDW	code	Bandwidth Code	Alphanumeric	25
BANDW	description	Bandwidth Description	Alphanumeric	256
CKTTYP	code	Access Circuit Type Code	Alphanumeric	6
CKTTYP	condition	Access Circuit Type Condition	Alphanumeric	50
CKTTYP	description	Access Circuit Type Description	Alphanumeric	256

Data Transaction Code	Element Name	Description	Data Type	Length
CNTRY	aow	Area of the World (AOW). Edit Mask: NNNNNN	Numeric	6
CNTRY	code	Country Code	Alphanumeric	10
CNTRY	comments	Comments	Alphanumeric	256
CNTRY	country	Country Description	Alphanumeric	50
CNTRY	iso_alpha_2	2-letter alphanumeric ISO country code	Alpha	2
CNTRY	iso_alpha_3	3-letter alphanumeric ISO country code	Alpha	3
CNTRY	iso_numeric_code	ISO Numeric Country Code. Edit Mask: NNN	Numeric	3
CNTRY	jurisdiction_ID	Country Jurisdiction ID. Edit Mask: NNNNNN	Numeric	6
CNTRY	postal_code_format	Format of postal code	Alphanumeric	10
CNTRY	postal_name	Postal Name	Alphanumeric	20
CNTRY	sovereign	Sovereign	Alpha	2
CRGFRQ	code	Charging Type Code	Alphanumeric	10
CRGFRQ	description	Charging Type Description	Alphanumeric	256
CRGUNT	code	Charging Unit Code	Alphanumeric	5

Data Transaction Code	Element Name	Description	Data Type	Length
CRGUNT	description	Charging Unit Description	Alphanumeric	256
DRSN	code	Dispute Reason Code	Alphanumeric	10
DRSN	description	Dispute Reason Description	Alphanumeric	256
DSTUS	code	Dispute Status Code	Alphanumeric	1
DSTUS	description	Dispute Status Description	Alphanumeric	256
DTT	code	Data Transaction Type Code	Alphanumeric	6
DTT	description	Data Transaction Type Description	Alphanumeric	256
JCKTYP	code	Access Jack Type Code	Alphanumeric	25
JCKTYP	condition	Access Jack Type Condition	Alphanumeric	50
JCKTYP	description	Access Jack Type Description	Alphanumeric	256
KPIAO	code	KPI AQI Operator	Alphanumeric	6
KPIAO	description	KPI AQI Operator Description	Alphanumeric	256
KPILQ	code	KPI Location Qualifier Code	Alphanumeric	6
KPILQ	description	KPI Location Qualifier Description	Alphanumeric	256
KPIMU	code	KPI Measurement Unit Code	Alphanumeric	6
KPIMU	description	KPI Measurement Unit Description	Alphanumeric	256

Data Transaction Code	Element Name	Description	Data Type	Length
KPISLQ	code	KPI Service Level Qualifier	Alphanumeric	6
KPISLQ	description	KPI Service Level Qualifier Description	Alphanumeric	256
KPIUC	code	KPI Unit Type Code	Alphanumeric	6
KPIUC	description	KPI Unit Type Description	Alphanumeric	256
LNECD	code	Line Coding Code	Alphanumeric	5
LNECD	condition	Line Coding Condition	Alphanumeric	50
LNECD	description	Line Coding Description	Alphanumeric	256
LOADEP	code	Letter of Agency Dependencies Code	Alphanumeric	4
LOADEP	description	Letter of Agency Dependencies Description	Alphanumeric	256
ORDHDR	code	Order Header Type Code	Alphanumeric	1
ORDHDR	description	Order Header Type Description	Alphanumeric	256
ORDITM	code	Order Item Type Code	Alphanumeric	1
ORDITM	description	Order Item Type Description	Alphanumeric	256
ORDREJ	code	Order Rejection Code	Alphanumeric	25
ORDREJ	description	Order Rejection Description	Alphanumeric	256
SVC	cbsa_based_service	Core-based Statistical Area (CBSA) Based Service (See Section C)	Alphanumeric	20

Data Transaction Code	Element Name	Description	Data Type	Length
SVC	mandatory_optional	Mandatory or Optional service (See B Section). Expected values: M or O	Alpha	1
SVC	section_b_reference	Section B Reference for this service (See Section B)	Alphanumeric	20
SVC	section_c_reference	Section C Reference for this service (See Section C)	Alphanumeric	20
SVC	service	Service (See Section B)	Alphanumeric	256
SVC	service_area	Service_Area (See Section B)	Alphanumeric	256
SVC	service_clin_prefix	Service CLIN Prefix (See B Section)	Alpha	2
SVC	service_code	Service Code (See B Section)	Alphanumeric	20
TRUFLS	code	True/False Code	Alphanumeric	1
TRUFLS	description	True/False Description	Alphanumeric	256
YESNO	code	Yes/No Code	Alpha	1
YESNO	description	Yes/No Description	Alphanumeric	256

J.3 Delegation of Procurement Authority

DPA

TO: Name of Ordering Contracting Officer

FROM: EIS Contracting Officer

DPA Email Address

SUBJECT: Delegation of Procurement Authority for Ordering Contracting Officer to Compete, Award and Administer Task Orders

REF: EIS Contracts

The purpose of this Delegation of Procurement Authority (DPA) is to ensure that the roles and responsibilities between the EIS Contracting Officer (the Procuring Contracting Officer, a/k/a "PCO") and the Agency Ordering Contracting Officer (OCO)* are clearly established. The authority granted to you under this DPA is limited to the EIS contracts and those task orders awarded and administered by you under the EIS contracts. You will act as the central point of contact under each task order you compete, award, or administer, and you are responsible for coordinating with the awarded contractor and the General Services Administration (GSA). You will perform all required task order award and administration functions subject to the following terms and conditions of this DPA:

1. **Compliance** – You are required to comply with the referenced EIS contracts terms and conditions (as modified to allow this DPA), the Federal Acquisition Regulation (FAR) and the applicable authorized agency supplement or exception thereto, applicable agency-specific statutes and policies, and the additional responsibilities defined in this DPA. Reporting requirements are not applicable to agencies exempt from public posting.
2. **Duration** – This DPA is effective until the expiration of the respective EIS contracts or completion and closeout of the resultant task orders, whichever is later. You are also required to maintain a valid certificate of appointment. However, if you change organizations this DPA is automatically revoked. The DPA cannot be re-delegated.

3. **Revocation** – GSA may revoke this DPA at any time for failure to comply with treaty, law, regulation, ethical standards, applicable federal acquisition policies and procedures, and this DPA.
4. **Scope Compliance** – Ensure that task order work is within scope and below the applicable cumulative contract ceiling for the EIS Program. The OCO will provide the Request for Proposal / Request for Quotation to the EIS PCO prior to issuance. The EIS PCO coordinates scope determinations with the EIS program team. Scope reviews can be completed in parallel with the OCO's task order acquisition activities but the RFP/RFQ may not be issued until the scope review has been completed and the RFP/RFQ has been determined in writing by GSA to be in scope. You must include a copy of this DPA in the RFP/RFQ. The EIS PCO (or designee) shall inform the OCO if the SOW/PWS contained within the RFP/RFQ is within scope and provide comments and recommended changes if necessary. Any changes to the SOW/PWS or expansion of the original requirement will require an additional scope review by the EIS PCO. Should the EIS PCO determine an EIS task order to be out of scope, the PCO will inform the OCO that the task order must be canceled.
5. **Administrative Reporting** – Upon award, OCOs are responsible for entering task order information into the Federal Procurement Data System – Next Generation (FPDS-NG).
6. **Inventory** – The OCO shall maintain an accurate inventory of all service acquired under its task order(s). A copy of the inventory and any modifications shall be provided to GSA upon request.

The OCO is responsible for complying with all EIS contract and FAR-based rules when competing, awarding and administering task orders. The following list of duties represents key areas of responsibility (the list is not all-inclusive):

Training – The OCO must complete the required training in Section G of the contract. A DPA shall not be issued to an OCO until he/she has completed the training.

Ordering – All task orders awarded under this DPA shall be placed directly by the OCO. Task order CLINs and pricing shall be structured in accordance with Section B of the contract. CORs may only place service orders after the OCO has issued a fully funded task order. The service orders must be within scope and not exceed the funding on the task order

Fair Opportunity – Ensure that all contractors are provided a fair opportunity (FO) to be considered in accordance with FAR 16.505, and authorized agency supplements or exceptions thereto, prior to task order award. Any exceptions to fair opportunity to be considered (“fair opportunity exceptions”) must be consistent with FAR 16.505 or authorized agency supplements or exceptions thereto or as otherwise required or allowed by statute. If a fair opportunity exception is taken, the OCO shall document the basis for the exception, and post it in accordance with 16.505. All FOs must include all existing requirements. Any subsequent requirements exceeding $3500 shall be competed unless an exception to FO is taken.

Billing – Billing shall be done in accordance with Section G of the contract.

Price Analysis and Audits – Perform and document price analysis (FAR 15.4) as appropriate in determining the overall task order price to be fair and reasonable, as well as respond to any related audits. The OCO is responsible for the fair and reasonable determination for all task order pricing. Task order CLINs and pricing shall not be submitted to GSA for a fair and reasonable price determination.

Funding – Verify that funding is available. Comply with appropriations law and financial policy. Ensure timely obligation of funds, and de-obligation and disposition of excess funds.

COR – If a Contracting Officer's Representative (COR) is assigned to perform order monitoring functions, you must ensure that the extent of their authority and responsibilities is clearly defined and agreed upon. It is a best practice to complete COR designations in writing and present them to the contractor in order to establish clear roles and responsibilities during task order administration. Ensure that any COR you designate is properly equipped, trained and qualified to handle those responsibilities pursuant to your agency policy.

Task Order Protests, Disputes and Claims – Receive and respond to task order protests, disputes and claims. All protests, disputes and claims resulting from any task order issued under this DPA shall be resolved by the OCO.

Monitor, Evaluate, and Report Contractor Task Order Performance – Assure contractor performance and support compliance with both task order and contract terms and conditions. Take appropriate action to maintain the government's rights. OCOs should conduct contractor performance evaluations IAW FAR 42.15, and applicable agency policies. Past performance ratings shall be entered into the Contractor Performance Assessment Reporting System (CPARS).

Prompt Payment – Ensure prompt payment of contractor invoices and prompt rejection of nonconforming invoices.

Task Order Closeout – Perform task order closeout IAW FAR 4.804 and provide the EIS PCO with a task order closeout completion statement and closeout modification.

Requests for Information – Respond to any requests for information pertaining to task orders awarded or administered by you including but not limited to: Freedom of Information Act requests, and inquiries/audits by Congress, Inspectors General, the Small Business Administration, the Government Accountability Office and GSA.

If you have any questions regarding this DPA, EIS, or our program in general, please feel free to contact the EIS program team at any time.

For more information about EIS, please visit our website at http://gsa.gov/portal/content/219379. There you will find links to copies of the contracts and other useful information, including various points of contact.

*OGP 4800.2I includes entities that are not federal agencies and do not have Ordering Contracting Officers. Therefore, GSA shall also recognize 'authorized officials' that have the authority to bind their specific entities.

J.4 Guidelines for Modifications to EIS Program Contracts

In order for the government to efficiently process modifications to the contract, submissions must be clearly structured and conform to certain requirements. The following items delineate these requirements. This section also defines requirements for submission of TO-specific pricing and catalog pricing submissions.

All modifications and their associated cover letters and supporting documentation shall be submitted electronically via GSA Systems.

All modification submissions shall be numbered in accordance with the "Submission Numbering Scheme" in Appendix A.

The contractor shall resubmit in its entirety the contract file(s) containing the lowest level numbered section(s) of its contract that contain(s) the change. Files shall retain the same names as found in the original contract but shall not include dates within the file name. File names already containing a date shall be changed if and when the file is modified and resubmitted. The change to these file names shall be limited to the removal of the date portion.

Files submitted may be compressed. All submissions and documentation shall be compatible with GSA's office software. Each individual file in the submission shall be digitally signed, at the government's request. (Note that each file within a compressed file shall also be digitally signed, at the government's request.)

All files containing an item affected by the modification shall be included in the submission. This includes files that contain references that need to be changed as a result of the proposed modification including table of contents, list of figures, list of tables, and Attachment J. The Executive Summary section is not required to be resubmitted in any modification unless requested by the government.

A vertical line, adjacent to a change, in the margin shall be used to indicate that a change has been made. Deletions shall be indicated by strike-through. Only those changes pertaining to the modification under consideration shall be marked. Indications of all prior changes must be removed (including any "hidden" changes in Microsoft Word) by "accepting" all changes (using the "Track Changes" tools in Microsoft Word).

For initial and interim submissions, the following header shall appear on the upper right hand side on each page of the entire file:

Contract Number

Modification Number[2] – Initial and interim submissions shall insert "To be determined." Once the modification is accepted, the government will provide the contractor with the modification number to be inserted.

Effective Date – Initial and interim submissions shall insert "To be determined." Once the modification is acceptable, the government and the contractor will mutually agree upon the effective date to be inserted by the contractor.

For initial and interim submissions, the following footer shall appear on the lower right hand side of each page of the entire file:

Submission number

Electronic file name

Once agreement has been reached, a clean copy (showing only current changes) of all of the files that are being modified shall be resubmitted. The submission number and electronic file name shall remain in the footer. The cover letter shall include a brief description of each proposed enhancement in plain, easily understood English for release to user agencies via the Internet to announce the enhancement or modification (see Appendix B Example). All communications via the GSA Systems Discussion Tool or email relative to submittal of proposed enhancements or modifications shall include the applicable submission number.

Upon receipt of a contractor's initial submission for a modification, GSA and the contractor will then negotiate and process the proposed contract modification using an issue list, working through and deleting open issues as part of the negotiation. When all open issues on the list have been closed, the contractor should submit a final submission.

Procedures and examples for updating the pricing tables are provided in Appendix C.

J.4.1 Task Order-Specific Pricing Submissions

A Task Order Unique CLIN (TUC) is a CLIN used to define and price services of a TO-unique nature. See Section B.1.2.2 for definition and use of TUCs. TUCs and pricing for TUCs are not added to the contract via contract modification but are incorporated into the contract databases for pricing and billing purposes.

All TO-specific pricing submissions must populate the TO number column of the respective price tables with a valid TO number. TO-specific pricing submissions shall only include TUC prices, prices for contract fixed and ICB CLINs where the prices have been established for a TO, and/or catalog device class discount tables where the percentage discounts from OLP have been established for a TO. Such pricing is only valid for orders placed under the associated TO number.

[2] Modification number is not required for TO-specific submissions or catalog submissions

A submission of this type shall not result in a contract modification including, but not limited to establishing new contract pricing and revising contract volumes.

TO-specific submissions shall follow the guidelines and adhere to the requirements for contract modifications described above with the addition of the following:

1. A TO-specific submission shall not contain descriptions of new services or new CLINs.
2. The cover letter for a TO-specific pricing submission shall include the agency's TO number.
3. A TO-specific price for a service that is identical to a service on contract (i.e., excluding ICB prices) shall be equal to or lower than the contract price for the identical service.
4. Upon receipt of a TO-specific pricing submission, GSA will check the submission for proper structure and formatting of the pricing tables and will advise the contractor if any corrections are needed. The contractor shall have ten (10) business days to submit a corrected price submission. When a correct submission is received and accepted, the TO-specific pricing will be integrated into GSA Systems and the contractor will be notified.
5. If an agency TO requires the definition of new CLINs not already on contract, the contractor must place those CLINs on contract via a contract modification prior to submitting TO-specific pricing for them.

J.4.2 Catalog Submissions

The contractor shall make catalog submissions in a timely manner to ensure synchronization between the contractor's online catalog offerings and GSA Systems.

A submission of this type shall not result in a contract modification including, but not limited to, establishing new contract pricing and revising contract volumes.

Catalog submissions shall follow the guidelines and adhere to the requirements for contract modifications described above with the addition of the following:

1. A catalog submission shall not contain descriptions of new services or new CLINs.
2. Upon receipt of a catalog submission, GSA will check the submission for proper structure and formatting and will advise the contractor if any corrections are needed. When a correct submission is received, the catalog data will be integrated into GSA Systems. GSA shall notify the contractor if there are issues with the data being integrated.

APPENDIX A

Submission Numbering Scheme

Contractors shall use the submission numbering scheme presented in this document. Contractors shall be responsible for assigning and maintaining submission numbers, and do not have to contact the government in order to generate a submission number. This scheme allows a single submission number to be used for several contractor submissions to the government that lead to a single contractor modification. The format of the complete scheme for coding submission numbers is as follows:

CCSSSSS.VVT, where:

| | | | |

| | | | Type of Proposed Submission (T, alpha)

| | | |

| | | Version Number (VV, numeric)

| | |

| | Submission Number (SSSSS, numeric)

| |

Contractor ID (CC, alphanumeric), as assigned by the government to indicate contractor.

Types of proposed submissions (“T”) include the following:

- “a” is any modification to the contract
- “c” is a catalog submission
- “t” is a TO-specific submission

Submission numbers (“SSSSS”) shall be five digits and shall be unique for each submission.

The version number (“VV”) is a two-digit version control number that begins with the value “01” and increases by 01 for each subsequent version. Using version numbers after the submission number allows for all correspondence generated for a single proposed contract modification, catalog submission, or TO-specific submission to have the same submission number.

The following examples demonstrate the proper use of the submission numbering scheme:

Example one: Company AA submits a proposed enhancement that requires four iterations to become a contract modification. The submission numbers are as follows:

AA00101.01a -> initial submission

AA00101.02a

AA00101.03a

AA00101.04a -> final submission that is accepted as a contract modification

Example two: Company BB submits a proposed price reduction that requires four iterations to become a contract modification. The submission numbers are as follows:

BB00101.01a -> initial submission

BB00101.02a

BB00101.03a

BB00101.04a -> final submission that is accepted as a contract modification

Note: It is the government's intent to keep and maintain logs of contract modification, catalog submission, and TO-specific submission activity using this submission numbering scheme.

MODIFICATION NUMBERING SCHEME

The modification number will consist of one alphabetical identifier followed by five alphanumerical identifiers, for example:

P: Issued by the Procuring Contracting Office (P00001)

A: Issued by the Administrative Contracting Office (A00001)

APPENDIX B

Example

The Submission Cover Letter for Contract Modifications must provide summary information as applicable.

The following files are included in this submission:

Submission Number	Technical (Volume I) Change Section	Management (Volume II) Change Section	Business (Volume III)	Price (Volume IV) Change Section	Contract Change Section	Pricing Table
Section Name	Internet Protocol Service Table of Contents	Access to Data and Information Service Ordering Trouble and Complaint Reporting Data Reporting Requirements Table of Contents	Proposal Notes	Pricing Overview Table of Contents	Section B	B.X.X.X B.X.X.X
File Name	v1_X-X-XX.doc v1-Contents.doc	v2_X-X,doc v2_X-X,doc v2_X-XX,doc v2_X-XX,doc v2-Contents.doc	V3-XX.doc	Narrative.doc V4-Contents.doc	Section B.doc	GSA Systems

The following is a summary of the changes contained in the submission:

- Volume I-Technical-Section X.X.XX.X entitled XXXXXXX was added on page 23 of the Internet Protocol Service of the contract.
- Volume II-Management-Section X.X.XX.X.X.X was added on pages 25-27 to identify responsibilities of the Service Operations Center, Trouble Reporting and Escalation Procedures. A statement regarding non-issuance of Trouble Status Reports was added to Table X.SS-S. XXXXXX has identified exceptions to the deliverable reporting data in Section X.SS and has acknowledged that information concerning are not integrated with the existing EISXXXXX systems.
- Volume III-Business-Section3, XXXXXX Service Terms and Conditions, has been updated to include the specific provisions for XXXXXX services.
- Volume IV-P-Table X.XX.X was added to show the feature XXXX Mechanisms and Feature Item Numbers for XXXX services.
- Price Table B.X.X-X and B.X.X-X were updated to include 27 CLINs for XXXX services.

APPENDIX C

Instructions for the Submission of Modifications

Overview

GSA Systems will use a relational database to maintain the up-to-date contract price information. Contractors will need to maintain a reliable relational database of the complete set of current prices that shall match with GSA Systems in terms of price and location tables, their formats and contents. The contractor shall maintain its connection to GSA Systems for the duration of the contract. The GSA Systems' database will be maintained by the government as its definitive repository of prices for the life of the EIS contract. The complete set of current prices shall include all prices in the contract including price changes due to contract modifications, plus prices resulting from approved TO-specific submissions and catalog submissions. The complete set of current contract prices will be used as the baseline for the preparation of proposed contract modifications that include potential future price changes to be included in the contract.

Proposed contract, TO-specific, and catalog prices:

- Shall exclude the GSA AGF
- Shall include all appropriate discounts
- Shall include the correct numerical precision (the correct number of digits after the decimal point)
- Shall not exceed those already on contract for the identical service

The term **submission** refers to a contractor-generated proposal for:

1. a contract modification,
2. a TO-specific submission, or
3. a catalog submission,

A successful contract modification submission will become a contract modification after the contracting officer's approval. At time of submission, the contractor will assign each submission a submission number in accordance with the "Submission Numbering Scheme" defined in Appendix A. Submissions that include more than one service may be delayed. The contractor shall submit contract modification submissions, TO-specific submissions, and catalog submissions, separately.

The contractor shall submit contract modification submissions, TO-specific submissions, and catalog submissions, (initial, interim and final) via GSA Systems.

Procedures

Submissions shall be incremental. That is, the submitted price change file will contain only tables that have been added or changed, and only rows within those tables that have been added, removed, or changed. Furthermore, any one submission shall contain only the changes for that one submission, not any combination of the current and previous submissions.

The contractor shall use a version number of "01" for the initial version of a submission. Subsequent versions of the submission shall not be incremental with respect to the previous version, but rather shall completely replace the previous version. The contractor shall ensure that any version submitted subsequent to the initial version is structured so that it contains a full and complete representation of the current state of the submission.

All price changes, price additions, and price deletions require the contractor to submit at least one row to each affected B-table. The submitted row(s) shall contain at a minimum the TO number[3], the CLIN, the price, the price start date and the price stop date.

All price tables include a price-replaced date column. This column is to be completed only by the government; the contractor shall not make an entry in the price replaced date column in its submissions. This column will remain NULL in all tables in the current contract schema (e.g. v0_eis). After award of any contract modification or approval of any TO-specific submission or catalog submission that changes a price table, the government will, as part of its process for integrating the awarded or approved price data, enter the date of execution into the price-replaced date column in all new rows created in the contract archive schema (e.g. v0_eis_archive).

Adding a New CLIN to an Existing Table[4]

To add a new CLIN to an existing table, the contractor must propose a contract modification to:

1. Define the new CLIN,

[3] For contract modification submissions, the contractor shall populate the TO Number column with "-1"

[4] New CLINs shall only be added via contract modification submissions, not via TO-specific submissions or catalog submissions

2. Identify which B-table the CLIN is in (and, if applicable, the location or combination of location values), and
3. Provide prices and effective dates for the new CLIN

To define the new CLIN, the contractor shall add a row in the “clin” table to define each new CLIN being added to the contract. The following are guidelines for defining a new CLIN:

- New CLIN descriptions should NOT contain the following:
  - Service ID or Service Name (e.g., PLS, Wireless, Voice Service)
  - Frequency (e.g., MRC, NRC, Usage)
- New CLIN descriptions should be structured and formatted like similar existing CLINs to aid users in distinguishing between similar, related CLINs. CLIN assignments should be chosen so that the CLINs of similar, related services fall within close proximity to one another in lists that are sorted by CLIN.

To define which B-table the CLIN is in (and, if applicable, the location or combination of location values) the contractor shall add a row in the “loc_base_input” table for each Btable_id for which the new CLIN is being added. For each new Btable_id, additional rows shall be added to indicate all valid location values or combinations of location values.

To provide the price(s) and effective dates for the new CLIN, the contractor shall submit at least one row for each affected B-table; the submitted row(s) shall contain a TO number of -1, the CLIN, the price for the CLIN, the price start date and the price stop date, along with any other parameters such as location values that are required for the B-table to fully differentiate the price.

Example

Table 1 represents the submission of the row to be added to the “clin” table to define a new CLIN. It includes the new CLIN, the description (name) of the new CLIN and several required characteristics of the CLIN.

clin	name	frequency	icb	nsp	unit_id	notes
MN11002	Managed Network Implementation, Maintenance and Management, Small	NRC	0	0	261	

Table 1: Submitted clin table

Table 2 shows the entry required in the “loc_base_input” table to identify the B-table(s) into which the new CLIN is to be inserted. This table defines CLIN MN11002 to be priced in Table B.2.8.1.3.1; the -1 entries in the loc1 and loc2 columns define that the CLIN is not location specific.

clin	btable_id	loc1	loc2
MN11002	28131	-1	-1

Table 2: Submitted loc_base_input table

Also, the TO number, CLIN, price(s), price start dates and price stop dates for the new CLIN must be added to the appropriate B-table(s). Table 3a below represents the state of the table prior to submission of the contract modification.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-09-30	
-1	MN11001	80	2019-10-01	2020-09-30	
-1	MN11001	60	2020-10-01	2027-09-30	

Table 3a: Contract B-table prior to Mod Submission

To add new CLIN MN11002 to the above table, with prices through the end of the contract, the contractor would submit the following table (Table 3b).

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11002	200	2017-10-01	2022-09-30	

Table 3b: Submitted B-table

This provides a price for the new CLIN from the price start date to the end of the first option period. Note that since this is a contract modification, not a TO-specific submission, the task order number column of the price table is populated with "-1".

After the contract modification is executed, the government will integrate the proposed modification. After integration of the modification, the revised Table B.2.8.1.3.1 would appear as shown below in Table 3c.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-09-30	
-1	MN11001	80	2019-10-01	2020-09-30	
-1	MN11001	60	2020-10-01	2022-09-30	
-1	MN11002	200	2017-10-01	2022-09-30	

Table 3c: Contract B-table After Mod Integration

Adding a New Price for an Existing CLIN to an Existing Table

To price an existing CLIN in an existing B-table, the contractor shall submit at least one pricing row for each affected B-table; the submitted row(s) shall contain the TO number[3], the CLIN, the price for the CLIN, the price start date and the price stop date, along with any other parameters such as location, that are required for that B-table to fully differentiate the price. If the CLIN has never been priced in the desired B-table, the contractor shall also include a "loc_base_input" table row in the submission for the B-table in which the CLIN is being priced for the first time.

Changing an Existing Price in a Table

To indicate a price change, the contractor shall submit new price rows to replace the existing prices. Note that all current and future dates covered by the replaced price row(s) shall be covered by the added row(s). That is, contractors shall take care not to create date “holes” in price coverage. Note that the new price shall be effective on the price start date.

Example

Table 4a below represents the state of the table prior to submission of the contract modification.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-09-30	
-1	MN11001	80	2019-10-01	2020-09-30	
-1	MN11001	60	2020-10-01	2022-09-30	
-1	MN11002	200	2017-10-01	2022-09-30	

Table 4a: Contract B-table prior to Mod Submissions

To reduce the price of CLIN MN11001 from the existing price of $100 to $90 for the period 2019-4-01 through 2019-09-30, the contractor would submit the following table with only one row as shown below (Table 4b).

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	90	2019-04-01	2019-09-30	

Table 4b: Submitted B-table

After award of the modification (e.g. the mod is executed on 2019-03-22), the government makes the necessary database adjustments to integrate the modification. After integration of the modification, the revised Table B.2.8.1.3.1 would appear as shown below (Table 4c). Notice that the government modified one row to change the

price stop date from 2019-09-30 to 2019-03-31 and then added a new row reflecting the price reduction, with a price start date of 2019-04-01.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-03-31	
-1	MN11001	90	2019-04-01	2019-09-30	
-1	MN11001	80	2019-10-01	2020-09-30	
-1	MN11001	60	2020-10-01	2022-09-30	
-1	MN11002	200	2017-10-01	2022-09-30	

Table 4c: Contract B-table After Mod Integration

In addition, the following would be added by the government to Table B.2.8.1.3.1 in the contract archive schema.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices (archive)

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-09-30	2019-03-22

Table 4d: Row Added to Archive B-table After Mod Integration

Adding a Task Order-Specific Price

The procedure for adding a TO-specific price is similar to that of adding a new price for an existing CLIN to an existing table. The difference is that the contractor shall populate the task order number column with a valid TO number rather than “-1”. For example, starting with Table 4c from above, the contractor could include the following Table 5a in a TO-specific submission.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
SS00-34-90186	MN11002	190	2019-05-01	2022-09-30	

Table 5a: Submitted B-table

After integration of the submission, the revised Table B.2.8.1.3.1 would appear as shown below (Table 5b).

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-03-31	
-1	MN11001	90	2019-04-01	2019-09-30	
-1	MN11001	80	2019-10-01	2020-09-30	
-1	MN11001	60	2020-10-01	2022-09-30	
-1	MN11002	200	2017-10-01	2022-09-30	
SS00-34-90186	MN11002	190	2019-05-01	2022-09-30	

Table 5b Contract: B-table After Task Order-Specific Submission Integration

Deleting a Price

To submit a price for deletion, the contractor shall include the row in the submission with the price start date and the price stop date both set to the last day of the month the CLIN will be available. Note that the last date the price shall be in effect is on the price stop date.

Example

Using Table 4c above as a starting point, if the contractor proposes to delete pricing for CLIN MN11001 effective at the end of calendar year 2021, the contractor would submit the following table with only one row as shown below (Table 6a).

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	60	2021-12-31	2021-12-31	

Table 6a: Submitted B-table

After award of the modification, the government makes the necessary database adjustments to integrate the modification. After integration of the modification, the new Table B.2.8.1.3.1 would appear as shown below (Table 6b). Notice that the government modified one row to change the price stop date from 2022-09-30 to 2021-12-31.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-03-31	
-1	MN11001	90	2019-04-01	2019-09-30	
-1	MN11001	80	2019-10-01	2020-09-30	
-1	MN11001	60	2020-10-01	2021-12-31	
-1	MN11002	200	2017-10-01	2022-09-30	

Table 6b: Contract B-table After Mod Integration

In addition, the following would be added by the government to Table B.2.8.1.3.1 in the contract archive schema.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices (archive)

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	60	2020-10-01	2022-09-30	(Mod Award Date)

Table 6c: Row Added to Archive B-table After Mod Integration

Adding a Catalog Item

The procedure for adding a catalog item is similar to that of adding a new price for an existing CLIN to an existing table. The difference is that the contractor shall populate the appropriate catalog tables. Below is an example of adding a catalog item for SRE associated with Device Class ID 6123. Other catalog items listed in Section B.1.3 should be added in similar fashion.

Table B.2.10.2.1: SRE Catalog – Product Specification Table

CLIN	Case Number	SRE Type	Manufacturer	Model No.	Part No.	UPC	Model/Part Description	Device Size	Rated for Energy Efficiency Compliance	Energy Efficiency Standards and Ratings	OLP	No List Price	Device Class ID	SRE MRC Options	Start Date	Stop Date	End of Sale Date	End of Life Date	Notes
EQ9000 1	0001	S	CISCO	N/A	CISCO1941W-A/K9		Cisco 1941 Router w/ 802.11 a/b/g/n FCC Compliant WLAN ISM	2	Y	EPEAT	$20905.00		6123	{24,36}	2019-10-01	2020-09-30			

Table 7a: Submitted B-table

Date Constraints

Price start and stop dates are not constrained to contract year boundaries. However, prices must start on the first day of a month and stop on the last day of a month. The price start date shall not be earlier than the date of the modification submission.

Adding a New Price Table

The format of a new price table must be reviewed and approved by the government prior to the submission of a modification. It should follow the basic guidelines of all current price tables, such as including columns for the TO number, CLIN, price, and start, stop and replace dates.

Submission Contents

All submissions must be submitted as specified below:

1) Tables in pre-approved price table formats
2) Tables stored in GSA Systems

At both the contractor's and the government's discretion, government resources may be made available to assist the contractor in the preparation of a submission (particularly, when a new price table format is involved). All proposals for contract modification

submissions, TO-specific submissions, and catalog submissions, that contain pricing data shall comply with these submission requirements; those that do not will be returned to the contractor unprocessed.

Verification Mechanism

The government will publish general reference information useful for preparing the price submission such as country/jurisdiction IDs, services, service types and categories, price table formats, valid start and stop dates, charging units, etc. The contractor shall reference this information before preparing its new submission to GSA. If the contractor needs any information that does not exist in the published material, such as country codes, charging units, or table formats, then GSA will provide that information.

The government may also provide pre-submission support to the contractor to verify its submission for correctness. This support consists of validating price tables (their names, table_ids, formats), price dates, and verifying new CLINs for uniqueness and details.

J.5 Labor Categories

All labor categories are based on the Office of Management and Budget's (OMB) Standard Occupational Classification (SOC), as supplemented by the Bureau of Labor Statistics (BLS) Department of Labor Employment and Training Administration's Occupational Information Network (O*NET) (http://online.onetcenter.org). More detailed information on each labor category, including required skills, knowledge, and tool experience, can be found on the O*NET website.

The SOC code is indicated for each labor category. Refer to section B.2.11.2, Labor Categories, for more information on the use of SOC codes in this contract. Also indicated for each labor category is the Occupational Group from the BLS Employment Cost Index to be used in determining price escalation factors. Refer to Section H.19 for information on labor price escalation.

The following labor categories are included in this contract.

Business Continuity Planner (SOC Code 13-1199.04; Occupational Group "Professional and related")

Develop, maintain, or implement business continuity and disaster recovery strategies and solutions, including risk assessments, business impact analyses, strategy selection, and documentation of business continuity and disaster recovery procedures. Plan, conduct, and debrief regular mock-disaster exercises to test the adequacy of existing plans and strategies, updating procedures and plans regularly. Act as a coordinator for continuity efforts after a disruption event.

Computer Network Architect (SOC Code 15-1143.00; Occupational Group "Professional and related")

Design and implement computer and information networks, such as local area networks (LAN), wide area networks (WAN), intranets, extranets, and other data communications networks. Perform network modeling, analysis, and planning. May also design network and computer security measures. May research and recommend network and data communications hardware and software.

Computer Network Support Specialist (SOC Code 15-1152.00; Occupational Group "Professional and related")

Analyze, test, troubleshoot, and evaluate existing network systems, such as local area network (LAN), wide area network (WAN), and Internet systems or a segment of a network system. Perform network maintenance to ensure networks operate correctly with minimal interruption.

Computer Systems Analyst (SOC Code 15-1121.00; Occupational Group "Professional and related")

Analyze science, engineering, business, and other data processing problems to implement and improve computer systems. Analyze user requirements, procedures, and problems to automate or improve existing systems and review computer system capabilities, workflow, and scheduling limitations. May analyze or recommend commercially available software.

Computer Systems Engineers/Architect (SOC Code 15-1199.02; Occupational Group "Professional and related")

Design and develop solutions to complex applications problems, system administration issues, or network concerns. Perform systems management and integration functions.

Customer Service Representatives (SOC Code 43-4051.00; Occupational Group "Service Occupations")

Interact with customers to provide information in response to inquiries about products and services and to handle and resolve complaints.

Database Administrator (SOC Code 15-1141.00; Occupational Group "Professional and related")

Administer, test, and implement computer databases, applying knowledge of database management systems. Coordinate changes to computer databases. May plan, coordinate, and implement security measures to safeguard computer databases.

Database Architect (SOC Code 15-1199.06; Occupational Group "Professional and related")

Design strategies for enterprise database systems and set standards for operations, programming, and security. Design and construct large relational databases. Integrate new systems with existing warehouse structure and refine system performance and functionality.

Electrical Drafter – Computer Aided Design (CAD) Operator (SOC Code 17-302.02; Occupational Group "Professional and related")

Prepare wiring diagrams, circuit board assembly diagrams, and layout drawings used for the manufacture, installation, or repair of electrical equipment.

Information Security Analyst (SOC Code 15-1122.00; Occupational Group "Professional and related")

Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses.

Information Technology Project Manager (SOC Code 15-1199.09; Occupational Group "Management, business, and financial")

Plan, initiate, and manage information technology (IT) projects. Lead and guide the work of technical staff. Serve as liaison between business and technical aspects of projects. Plan project stages and assess business implications for each stage. Monitor progress to assure deadlines, standards, and cost targets are met.

Network and Computer Systems Administrator (SOC Code 15-1142.00; Occupational Group "Professional and related")

Install, configure, and support an organization's local area network (LAN), wide area network (WAN), and Internet systems or a segment of a network system. Monitor network to ensure network availability to all system users and may perform necessary maintenance to support network availability. May monitor and test Web site performance to ensure Web sites operate correctly and without interruption. May assist in network modeling, analysis, planning, and coordination between network and data communications hardware and software. May supervise computer user support specialists and computer network support specialists. May administer network security measures.

Software Developer – Applications (SOC Code 15-1132.00; Occupational Group "Professional and related")

Develop, create, and modify general computer applications software or specialized utility programs. Analyze user needs and develop software solutions. Design software or customize software for client use with the aim of optimizing operational efficiency. May analyze and design databases within an application area, working individually or coordinating database development as part of a team. May supervise computer programmers.

Software Developer – Systems Software (SOC Code 15-1133.00; Occupational Group "Professional and related")

Research, design, develop, and test operating systems-level software, compilers, and network distribution software for medical, industrial, military, communications, aerospace, business, scientific, and general computing applications. Set operational specifications and formulate and analyze software requirements. May design embedded systems software. Apply principles and techniques of computer science, engineering, and mathematical analysis.

Software Quality Assurance Engineer/Tester (SOC Code 15-1199.01; Occupational Group "Professional and related")

Develop and execute software test plans in order to identify software problems and their causes.

Sustainability Specialist (SOC Code 13-1199.05; Occupational Group "Professional and related")

Address organizational sustainability issues, such as waste stream management, green building practices, and green procurement plans.

Telecommunications Engineering Specialist (SOC Code 15-1143.01; Occupational Group "Professional and related")

Design or configure voice, video, and data communications systems. Supervise installation and post-installation service and maintenance.

Telecommunications Equipment Installer/Repairer (SOC Code 49-2022.00; Occupational Group "Service Occupations")

Install, set-up, rearrange, or remove switching, distribution, routing, and dialing equipment used in central offices or headends. Service or repair telephone, cable television, Internet, and other communications equipment on customers' property. May install communications equipment or communications wiring in buildings.

Telecommunications Line Installer/Repairer (SOC Code 49-9052.00); Occupational Group "Service Occupations")

Install and repair telecommunications cable, including fiber optics.

Web Administrators (SOC Code 15-1199.03; Occupational Group "Professional and related")

Manage web environment design, deployment, development and maintenance activities. Perform testing and quality assurance of websites and web applications.

Web Developers (SOC Code 15-1134.00; Occupational Group "Professional and related")

Design, create, and modify Web sites. Analyze user needs to implement Web site content, graphics, performance, and capacity. May integrate Web sites with other computer applications. May convert written, graphic, audio, and video components to compatible Web formats by using software designed to facilitate the creation of Web and multimedia content.

J.6 GSA CIO IT Security Guides

GSA CIO Security Guides.zip

J.7 GSA IT Security Directives and Instructional Letters

GSA CIO Security Directives and Instruc

J.8 Security Assessment Document Templates

Security Assessment Document Templates

J.9 Site Survey Estimate Template for Wiring Install

Site Survey Estimate Template for Wiring Install*							**Version 1.0**
Quote Date:							
Quote Expiration Date:							
Service Location:							
Location ID: (include NSC)							
Contractor:							
Solicitation and/or Task Order No.:							
Install Description (Demarc Extension, New install, etc.)							
Attach Drawing, if applicable							
Attach Quote, if applicable							
Construction and Equipment Costs*							
Service/Product	**Description**	**Manufacturer/Part Number, Labor Category, where applicable**	**Qty**	**Unit (feet, hours, etc.)**	**Unit Price**	**Total**	**Price Source, if applicable**
Cable/Fiber (list type, strands, length)							
Conduit/Duct (list type and length)							
Installation - (Per Foot)							
Plowing							
Directional Boring - (Rural, Urban, Rock)							
Hand holes							

Hand hole Installation							
Firewall Penetration							
Equipment/Material							
Add Itemized Materials as needed							
Labor and Other Costs*							
Service/Product	**Description**	**Manufacturer/Part Number, Labor Category, where applicable**	**Qty**	**Unit (feet, hours, etc.)**	**Unit Price**	**Total**	**Price Source, if applicable**
List Labor Categories**, hours, and work to be performed							
Permits							
Other Incidental Elements that may contribute to price (provide detail)							
Total Estimated Project Cost							

* Categories may be left blank, modified, or added to provide a detailed estimate sufficient to support a fair and reasonable determination
** To the extent possible, include labor categories and rates from Section B.2.11

J.10 Site Survey Estimate Template for Special Access Construction

Site Survey Estimate Template for Special Access Construction*							**Version 1.0**
Quote Date:							
Quote Expiration Date:							
Service Location:							
Location ID: (include NSC)							
Contractor:							
Solicitation and/or Task Order No.:							
Type of Service (DS3, OC3, Ethernet, etc.)							
Attach Drawing							
Attach Contractor Quote							
Construction and Equipment Costs*							
Service/Product	**Description**	**Manufacturer/Part Number, Labor Category, where applicable**	**Qty**	**Unit (feet, hours, etc.)**	**Unit Price**	**Total**	**Price Source, if applicable**
Cable/Fiber (list type, strands, length)							
Conduit/Duct (list type and length)							
Installation - (Per Foot)							
Plowing							
Directional Boring - (Rural, Urban, Rock)							
Hand holes							

Hand hole Installation							
Equipment (FW4100 ES, Fiber Distribution Panel, NIUs, etc.)							
Equipment Rentals							
Additional Equipment (provide detail)							
Labor and Other Costs*							
Service/Product	**Description**	**Manufacturer/Part Number, Labor Category, where applicable**	**Qty**	**Unit (feet, hours, etc.)**	**Unit Price**	**Total**	**Price Source, if applicable**
List Labor Categories**, hours, and work to be performed							
Design							
Permits							
Traffic Control							
Mobilization							
Engineering							
Administration							
Other Incidental Elements that may contribute to price (provide detail)							
Total Estimated Project Cost							

* Categories may be left blank, modified, or added to provide a detailed estimate sufficient to support a fair and reasonable determination

** To the extent possible, include labor categories and rates from Section B.2.11

J.11 Abbreviations and Acronyms

J.11.1 Abbreviations and Acronyms Table

Abbreviation or Acronym	Definition
A	
A&A	Assessment and Authorization
AA	Access Arrangement
ACO	Administrative Contracting Officer
ACS	Audio Conferencing Service
ACT	Accounting Control Transaction
AD	Agency Dispute
ADSL	Asymmetric DSL
AGF	Associated Government Fee
AGFD	AGF Detail
AHC	Agency Hierarchy Code
AHS	Application Hosting Services
AIS	Automated Information System
ANI	Automatic Number Identification
ANSI	American National Standards Institute
Anti-DDoS	Anti-Distributed Denial of Service
AO	Authorizing Official
AOW	Area of the World
API	Application Programming Interface
APS	Automatic Protection Switching
ARIN	American Registry for Internet Numbers
AQL	Acceptable Quality Level
AS	Autonomous System
ASC	Accredited Standards Committee
ASCII	American Standard Code for Information Interchange
ASCO	Adversarial Supply Chain Operation
ASON	Automatic Switched Optical Network
ASP	Applications Services Provider
ASRN	Agency Service Request Number

Abbreviation or Acronym	Definition
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
ATO	Authority to Operate
ATR	AGF Electronic Funds Transfer Report
AU	Authorized Users
AUP	Acceptable Use Policy
Av(S)	Availability (Service)
AVI	Audio Visual Interleave
AVM	Anti-Virus Management
AVMS	Anti-Virus Management Service
B	
B2B	Business to Business
BA	Billing Adjustment
BI	Billing Invoice
BER	Bit Error Rate
BGAN	Broadband Global Area Network
BGP	Boarder Gateway Protocol
BIA	Business Impact Assessment
BIT	Binary Digit
BLS	Bureau of Labor Statistics
BoD	Bandwidth on Demand
BLSR	Bidirectional Line Switched Ring
BPS	Bits per second
BPSR	Bidirectional Path Switched Ring
BRI	Basic Rate Interface
BSD	Boundary Scope Document
BSS	Broadband Switching System
BSS	Business Support System
BTN	Billing Telephone Number
BYOD	Bring Your Own Device
C	
CA	Criticality analysis

Abbreviation or Acronym	Definition
CAC	Common Access Card
CAGE	Commercial and Government Entity
CAP	Compliance and Assurance Program
CBR	Constant Bit Rate
CBS	Committed Burst Size
CBSA	Core Based Statistical Area
CCCS	Customer Contact Center Services
CCE	Common Configuration Enumerations
CCS	Contact Center Service
CCV	Cybersecurity Compliance Validation
CDIP	Contractor Data Interaction Plan
CDMA	Code Division Multiple Access
CDN	Content Delivery Network
CDNS	Content Delivery Network Service
CDP	Carbon Disclosure Project
CDR	Call Detail Record
CDRL	Contract Deliverables Requirements List
CE	Customer Edge
CFR	Code of Federal Regulations
CFSS	Commercial Fixed Satellite Service
CGI-Bin	Common Graphic Interface - Binary
CID	Caller ID
CIR	Committed Information Rate
CIRs	Committed Information Rates
CIS	Center for Internet Security
CLIN	Contract Line Item Number
CLLI	Common Language Location Identifier
CLONES	Central Location Online Entry System (iconectiv database)
CMSS	Commercial Mobile Satellite Service
CNAM	Calling Name
CNM	Customer Network Management
CNSS	Committee on National Security Systems

Abbreviation or Acronym	Definition
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CO	Contracting Officer
COMSATCOM	Commercial Satellite Communication
CONUS	Continental United States
COOP	Continuity of Operations
COR	Contracting Officer's Representative
CoS	Class of Service
CoSS	Collaboration Support Services
COTS	Commercial off-the-shelf
CP	Contingency Plan
CPDF	Central Personnel Data File
CPE	Customer Premises Equipment
CPLG	Coupling
CPMO	Contractor's Program Management Office
CPTP	Contingency Plan Test Plan
CPTPR	Contingency Plan Test Plan Report
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSA	Communications Service Authorization
CSC	Customer Service Center
CSDS	Circuit Switched Data Service
CSO	Customer Support Office
CSP	Communications Service Provider
CSRN	Contractor Service Request Number
CSS	Circuit Switched Service
CSTA	Computer Supported Telephony Applications
CSU/DSU	Channel Service Unit/Data Service Unit
CSV	Comma-Separated Value
CSVS	Circuit Switched Voice Service
CTI	Computer Telephony Integration
CUI	Controlled Unclassified Information

Abbreviation or Acronym	Definition
CVE	Common Vulnerabilities and Exposures
CW	Cable and Wiring
CWD	Customer Want Date
D	
D/A	Departments and Agencies
DBA	Doing Business As
DBAS	Direct Billed Agency Setup
DCC	Data Communications Channel
DCOM	Distributed Component Object Model
DCS	Data Center Service
DCSS	Digital Cross-Connect Systems
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DFS	Dark Fiber Service
DHCP	Dynamic Host Configuration Protocol
DHS	Dedicated Hosting Service
DID	Direct Inward Dial
DIS	Draft International Standard
DLCI	Data Link Connection Identifier
DLP	Data Loss Prevention
DLS	Data Link Switching
DM	Degraded Minutes
DMS	Defense Message System
DMZ	Demilitarized Zones
DNBH	During Normal Business Hours
DNI	Dialed Number Identification
DNIS	Dialed Number Identification Service
DNS	Domain Name System
DNSSEC	DNS Security Extensions
DoD	Department of Defense
DoDI	Department of Defense Instruction
DoS	Denial of Service

Abbreviation or Acronym	Definition
DPA	Delegation of Procurement Authority
DR	Disaster Recovery
DR	Dispute Report
DSL	Digital Subscriber Line
DSN	Defense Switched Network
DSSR	Department of State Standardized Regulations
DSU	Data Service Unit
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-Frequency
DUNS	Data Universal Numbering System
DWDM	Dense Wavelength Division Multiplexing
E	
EAD	Enterprise Active Directory
ECS	Electronic Commerce Service
EFMA	Ethernet in the First Mile Alliance
EFS	Error Free Seconds
EFT	Electronic Funds Transfer
E-Gov	Electronic Government
EIA	Electronic Industries Association
EIA/TIA	Electronic Industry Alliance/Telecommunications Industry Association
EIS	Enterprise Infrastructure Solutions
EIT	Electronic and Information Technology
E-LAN	Ethernet Private Local Area Network
E-LINE	Ethernet Private Line
EM	Element Manager
EMI	Electro-Magnetic Interference
EMS	Element Management Systems
EN	Event Notification
EO	Executive Order
EP	Emergency Preparedness
EPA	Environmental Protection Agency
ERM	E-mail Response Management

Abbreviation or Acronym	Definition
ERP	Enterprise Resource Planning
ESCON	Enterprise System Connection
ESF	Extended Superframe
ESI	Electronically Stored Information
ETL	Extract, Transform and Load
ETS	Ethernet Transport Service
ETSI	European Telecommunications Standards Institute
EVC	Ethernet Virtual Connection
F	
FAR	Federal Acquisition Regulation
FB	Fixed Bandwidth
FCC	Federal Communications Commission
FCCI	Federal Cloud Computing Initiative
FCIA	Fiber Channel Industry Association
FDCCI	Federal Data Center Consolidation Initiative
FDP	Fiber Distribution Panel
FEDBIZOPPS	Federal Business Opportunities
FedRAMP	Federal Risk and Authorization Management Program
FED-STD	Federal Standard
FedVRS	Federal Video Relay Service
FEMP	Federal Energy Management Program
FICON	Fiber Connectivity
FIPS	Federal Information Processing Standard
FIPS 200	Federal Information Processing Standards Publication 200
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
FLSA	Fair Labor Standards Act
FOC	Firm Order Commitment
FOCN	Firm Order Commitment Notice
FOIA	Freedom of Information Act
FS	Federation Services
FSDP	Fiber Service Delivery Point

Abbreviation or Acronym	Definition
FT1	Fractional T1
FT3	Fractional T3
FTP	File Transfer Protocol
FTR	Federal Telecommunications Recommendations
FTTP	Fiber to the Premises
FUSF	Federal Universal Service Fund
G	
GAO	General Accounting Office
GB	Gigabyte
Gbps	Gigabit per second
GETS	Government Emergency Telecommunications Service
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFP	Government Furnished Property
GFP	Generic Framing Procedure
GMPLS	Generalized Multi-Protocol Label Switching
GOS	Grade of Service
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GRI	Global Reporting Initiative
GSA	General Services Administration
GSAR	GSA Regulation
GUI	Graphical User Interface
H	
HCM	Human Capital Management
HF	High Frequency
HIDS	Host-based IDS
HR	Human Resources
HSPD-12	Homeland Security Presidential Directive-12
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol

Abbreviation or Acronym	Definition
HVAC	Heating, Ventilation and Air Conditioning
I	
IA	Interagency Agreement
IaaS	Infrastructure as a Service
ICB	Individual Case Basis
ICE	Interactive Connectivity Establishment
ICMP	Internet Control Message Protocol
ID	Identification (User)
IDC	Internet Data Center
IDE	Integrated Development Environment
IDPS	Intrusion Detection and Prevention Service
IDS	Intrusion Detection System
IDSL	ISDN DSL
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IETF RFC	IETF Request for Comment
IMAP	Internet Message Access Protocol
INRS	Incident Response Service
IP	Internet Protocol
IPFIX	IP Flow Information Export
IPMS	Integrated Performance Monitoring Service
IPS	Internet Protocol Service
IPSec	IP Security
IPS	Intrusion Prevention Systems
IPSS	Intrusion Prevention Security Service
IPVS	Internet Protocol Voice Service
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IR1-SLM	Intermediate Reach Single Longitudinal Mode
IR	Inventory Reconciliation
IRP	Incident Response Plan

Abbreviation or Acronym	Definition
IRS	Internal Revenue Service
IRU	Indefeasible Rights of Use
ISA	Interconnection Security Agreements
ISCM	Information Security Continuous Monitoring
ISDN	Integrated Services Digital Network
ISDN BRI	ISDN Basic Rate Interface
ISM	In-Service Monitoring
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSM	Information Systems Security Manager
ISSO	Information System Security Officer
ISV	Independent Software Vendor
ITIL	IT Infrastructure Library
ITS	Integrated Technology Services
ITSM	IT Service Management
ITT	Information Technology Tools
ITU	International Telecommunications Union
ITU-TSS	International Telecommunications Union-Telecommunications Service Sector
IVR	Interactive Voice Response
K	
KPI	Key Performance Indicator
L	
L2TP	Layer 2 Tunneling Protocol
L3VPN	Layer 3 Virtual Private Network
LAN	Local Area Network
Latency(S)	Latency (Service)
LCAS	Link Capacity Adjustment Scheme
LDAP	Lightweight Directory Access Protocol
LEC	Local Exchange Carrier
LGC	Local Government Contact
LH	Long Haul
LLDS	Link Layer Data Service

Abbreviation or Acronym	Definition
LNP	Local Number Portability
LOA	Letter of Authorization
LOH	Line Overhead
LR1-SLM	Long Reach Single Longitudinal Mode
LSA	Local Service Agreement
LSP	Label Switched Paths
LTE	Long Term Evolution
M	
M2M	Machine to Machine
MACD	Moves, Adds, Changes, Disconnects
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MAS	Mobile Application Store
MB	Megabyte
MBI	Minimum Background Investigation
Mbps	Megabit per second
MBS	Maximum Burst Size
MCM	Mobil Content Management
MDM	Mobile Device management
MEF	Metro Ethernet Forum
MFS	Managed Firewall Service
MIL-STD	Military Standard
MIME	Multipurpose Internet Mail Extensions
MLPP	Multi-Level Precedence and Preemption
MMC	Monthly Maintenance Charge
MMF	Multi-Mode optical Fiber
MMRC	Maintenance Monthly Recurring Cost
MMS	Multimedia Messaging Service
MNS	Managed Network Service
MOS	Mean Opinion Score
MPIN	Marketing Partner Identification Number
MPLS	Multi-Protocol Label Switching

Abbreviation or Acronym	Definition
MPS	Managed Prevention Service
MRC	Monthly Recurring Charges
MRG	Minimum Revenue Guarantee
MS	Microsoft
MSS	Managed Security Service
MTIPS	Managed Trusted Internet Protocol Service
MTTLBCI	Mean Time to Loss of BCI
MUX	Multiplexer
MWS	Wireless Service
N	
NACI	National Agency Check with Written Inquiries
NACSZ	Name, Address, City, State, Zip code
NAICS	North American Industry Classification System
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NCPS	National Cyber Protection System Sensor
NCS	National Communications System
NDA	Non-Disclosure Agreement
NEBS	Network Equipment-Building System
NFC	Near Field Communication
NFS	Network File Systems
NFV/SDN	Network Function Virtualization and Software Defined Network
NIC	Network Interface Card
NIDS	Network Intrusion Detection Devices
NIS	Network Information Service
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NLT	Not Later Than
NMS	Network Management System
NNI	Network to Network Interface
NOC	Network Operations Center

Abbreviation or Acronym	Definition
NPA	Numbering Plan Area
NPA/NXX	Numbering Plan Area / Numbering Plan Exchange
NRC	Non-Recurring Charge
NS	National Security
NS/EP	National Security and Emergency Preparedness
NS2020	Network Services 2020
NSA	National Security Agency
NSC	Network Site Code
NSP	Not Separately Priced
NTSC	National Television Standards Committee
NUI	Network User Identification
NVF	Network Function Virtualization
NXX	Numbering Plan Exchange
NZDS	Non-Zero Dispersion Shifted
O	
O&S	Operations and Support
O*NET	Occupational Information Network
OADM	Optical Add-Drop Multiplexer
OAM	Operations, Administration and Management
OAM&P	Operations, Administration, Maintenance and Provisioning
OCN	Operating Company Number
OCO	Ordering Contracting Officer
OCONUS	Outside Contiguous United States
OCWR	Optical Continuous Wave Reflectometry
OEC	Office of Emergency Communication
OEM	Original Equipment Manufacture
OFCS	Optical Fiber Communications System
OFSTP	Optical Fiber System Test Procedure
OIF	Optical Internetworking Forum
OLP	Official List Price
OMB	Office of Management and Budget
ONBH	Outside Normal Business Hours

Abbreviation or Acronym	Definition
OOS	Out-Of-Service
OPM	Office of Personnel Management
OS	Operating System
OSAISO	Office of the Senior Agency Information Security Officer
OTDR	Optical Time-Domain Reflectometer
OTM	Optical Terminal Multiplexer
OTN	Optical Transport Network
OVF	Open Virtualization Format
OVPN	Optical Virtual Private Network
OWS	Optical Wavelength Service
P	
P&P	Policies and Procedures
PaaS	Platform as a Service
PAL	Phase Alternation by Line
PAT	Port Address Translation
PBX	Private Branch Exchange
PC	Personal Computer
PCL	Physical Concentration Location
PDF	Portable Document Format
PDU	Protocol Data Unit
PHub	Pricing Hub
PIA	Privacy Impact Assessment
PIC	Presubscribed Interexchange Carrier
PIDF	Presence Information Data Format
PII	Personally Identifiable Information
PIID	Procurement Instrument Identifier
PIM	Personal Information Management
PIN	Personal Identification Number
PIR	Peak Information Rate
PIV	Personal Identity Verification
PKI	Public Key Encryption
PLS	Private Line Service

Abbreviation or Acronym	Definition
PM	Performance Monitoring
PMD	Polarization Mode Dispersion
PMO	Program Management Office
PMP	Program Management Plan
POA&M	Plan of Action and Milestones
POC	Point of Contact
PoE	Power over Ethernet
PON	Passive Optical Networks
POP	Point of Presence
PPIRS	Past Performance Information Retrieval System
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
PRI	Primary Rate Interface
PS/ALI	Private Switch/Automatic Location Identification
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTT	Push to Talk
PVC	Permanent Virtual Circuit
PWE	Pseudo Wire Emulation
PWE3	Pseudo Wire Emulation Edge to Edge
PWS	Performance Work Statement
Q	
QA	Quality Assurance
QoS	Quality of Service
QPMR	Quarterly Program Management Review
R	
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
RFC	Request for Comment
RFI	Request for Information
RFI	Radio Frequency Interference
RFP	Request for Proposal

Abbreviation or Acronym	Definition
RFQ	Request for Quotation
RMF	Risk Management Framework
RoB	Rules of Behavior
RPC	Remote Procedure Call
RPR	Resilient Packet Rings
RT	Response Time
RTP	Real-Time Transport Protocol
RTT	Radio Transmission Technology
S	
SaaS	Software as a Service
SAM	System for Award Management
SAN	Storage Area Networks
SAR	Security/Risk Assessment Report
SC(O)	Switched Connection (Optical)
SCAP	Security Content Automation Protocol
SCCP	Skinny Client Control Protocol
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCOM	System Center Operations Manager
SCRM	Supply Chain Risk Management
SD	Signal Degradation
SDH	Synchronous Digital Hierarchy
SDK	Software Development Kit
SDN	Software Defined Network
SDP	Service Delivery Point
SDS	Switched Data Service
SDSL	Symmetric DSL
SECAM	Système Electronique Couleur Avec Memoire
SES	Severely Errored Seconds
SF	Super Frame
SF	Signal Failure
SFTP	Secure File Transport Protocol

Abbreviation or Acronym	Definition
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SIS	Satellite Internet Service
SLA	Service Level Agreement
SLACR	SLA Credit Request
SLACRR	SLA Credit Request Response
SLAR	SLA Report
SMB	Server Message Block
SME	Subject Matter Expert
SMF	Single Mode optical Fiber
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SO	Service Order
SOA	Service Order Acknowledgement
SOAC	Service Order Administrative Change
SOC	Security Operations Center; Service Order Confirmation
SOCN	Service Order Completion Notice
SORN	Service Order Rejection Notice
SOH	Section Overhead
SONET	Synchronous Optical Network
SONET ADM	SONET Add-Drop Multiplexer
SOO	Statement of Objective
SOW	Statement of Work
SP	Special Publication
SR	Short Reach
SRE	Service Related Equipment
SRG	Security Requirements Guide
SR-MLM	Short Reach Multi-Longitudinal Mode
SS	Storage Service
SSCN	Service State Change Notice
SSH	Secure Shell
SSL	Secure Sockets Layer

Abbreviation or Acronym	Definition
SSL/TLS	Secure Sockets Layer/Transport Layer Security
SSM	Synchronous Status Messaging
SSP	System Security Plan
STP	Shielded Twisted Pair
STUN	Session Traversal Utilities for NAT
SVC	Switched Virtual Circuit
SWC	Serving Wire Center
SWOT	Strengths, Weaknesses, Opportunities and Threats
T	
TACACS	Terminal Access Controller Access Control System
TAX	Tax Detail
TB	Terabyte
TBD	To Be Determined
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Telecommunications Device for the Deaf
TDD/TTY	Telecommunications Device for the Deaf/Teletypewriter
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TEMS	Telecommunications Expense Management Service
TESP	Telecommunications Electric Service Priority
TFS	Toll Free Service
TICAP	Trusted Internet Connection Access Provider
TIC	Trusted Internet Connection
TIN	Taxpayer Identification Number
TLS	Transport Layer Security
TMSAD	Trust Model for Security Automation Data
TO	Task Order
TOH	Transport Overhead
TOPP	Task Order Project Plan
TP	Transition Plan
TSGR	Transport Systems Generic Requirements
TSMP	Transition Strategy and Management Plan

Abbreviation or Acronym	Definition
TSP	Telecommunications Service Priority
TS/SCI	Top Secret/Sensitive Compartmented Informaiton
TTR	Time to Restore
TUC	Task Order Unique CLIN
U	
UBI	Unique Billing Identifier
UCS	Unified Communications Service
UI	User Interface
UIFN	Universal International Free Phone Number
UM	Unified Messaging
UMTS	Universal Mobile Telecommunications System
UNI	User-to-Network Interface
UPS	Uninterruptible Power System
UPSR	Unidirectional Path Switched Ring
URL	Universal Resource Locator
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team
USDA	United States Department of Agriculture
UTC	Coordinated Universal Time
UTP	Unshielded Twisted Pair
V	
V&H	Vertical and Horizontal
VBR	Variable Bit Rate
VESDA	Very Early Smoke Detection Apparatus
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VoIPTS	Voice over Internet Protocol Transport Service
VPAT	Voluntary Product Accessibility Template
VPN	Virtual Private Network
VPNS	Virtual Private Network Service
VS	Voice Service
VSAT	Very Small Aperture Terminal

Abbreviation or Acronym	Definition
VSR	Very Short Reach
VSS	Vulnerability Scanning Service
VT	Virtual Tributary
VTN	Virtual Telephone Number
VTS	Video Teleconferencing Service
VXML	Voice Extensible Markup Language
W	
WAN	Wide Area Network
WAP	Wireless Application Protocol
WCS	Web Conferencing Service
WDM	Wavelength Division Multiplexing
WEP	Wired Equivalent Privacy
WFM	Workforce Management
WLAN	Wireless Local Area Network
WMI	Windows Management Instrumentation
WPA	Wi-Fi Protected Access
WPS	Wireless Priority Service
WSDL	Web Service Definition Language
WWW	World Wide Web
X	
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
XSD	XML Schema Definition
XTACACS	Extended TACACS

J.12 Glossary of Terms

12x5 Support - Shall include the core hour coverage of 8AM – 7PM Eastern Time Monday – Friday
24x7 - Twenty-four hours a day, seven days a week, without exception (e.g., national holidays are not excluded).
3rd Generation Partnership Project (3GPP) - An agreement formed in December 1998 by several telecommunications standard bodies to create technical specifications for the International Telecommunication Union's third-generation standards; represented in the group are companies from China, Europe, Japan, Korea, and the United States.
Acceptable Quality Level (AQL) - The performance level guaranteed by the contractor for each KPI associated with an EIS service.
Access - The facility-based service arrangements that provide net locations and their associated points of connection with the transport service providers, known as Points of Presence (POPs).
Access Circuit - A dedicated facility, varying by type (e.g., analog, digital signal, or synchronous optical network) and by bandwidth, used to carry service(s) between an SDP and its POP.
Access Control - The process of limiting access to the resources of a system only to authorized personnel, programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.
Access Type - The type of access being provided. Five access types are defined for EIS: 1. Wireline Access, 2. Ethernet Access, 3. Cable Access, 4. Fiber to the Premises (FTTP), 5. Wireless Access.
Ad Hoc Reporting - The generation of reports at sporadic intervals with varying contents and purposes.
Advanced Encryption Standard (AES) - Symmetric key cryptographic standard published by NIST. Uses 128, 192, or 256 bit keys. Designed as replacement for DES.
Agency - An organizational entity of the United States Federal Government. Also used in this document to refer to any entity authorized to purchase EIS services.
Agency Hierarchy Code (AHC) - A unique 28-character internal government accounting code that must be tracked for all services from order submission through disconnection.
Agency Locations - The physical address of agencies, sub-agencies, or other authorized users of EIS services.
Agency Service Request Number (ASRN) - Agency-provided service request number.
Alliance for Telecommunications Industry Solutions (ATIS) - A North American organization, formerly called ECSA, established to develop standards and guidelines for the methods and procedures needed in the telecommunications industry. ATIS has four committees, T1, SONET, Internet Work Interoperability Test Coordination, and Order and Billing Form.

Alphanumeric - Any of the 26 upper-case alphabetic letters (A through Z) and 10 numerals only (0 through 9).
Alternate Mark Inversion (AMI) - A line coding method used in T-1 and other digital wire transmission systems.
American National Standards Institute (ANSI) - The US organization that sets the rules and procedures for, and also authorizes specific standards setting organizations. ATIS and EIA/TIA are two ANSI authorized standards setting organizations in the US in the subject area of telecommunications.
American Standard Code for Information Interchange (ASCII) - The standard code used for information interchange among data processing systems, data communications systems, and associated equipment in the United States.
Americans with Disabilities Act (ADA) - Public Law 101-336 (Public Law 336 of the 101st Congress), enacted July 26, 1990). The ADA prohibits discrimination and ensures equal opportunity for persons with disabilities in employment, State and local government services, public accommodations, commercial facilities, and transportation. It also mandates the establishment of TDD/telephone relay telecommunications services.
Application Programming Interface (API) - A software program that has defined information entry and exit points in that allows other programs or devices to communicate with the software program.
Associated Government Fee (AGF) Structure - The structure for calculating the AGF presented by GSA to the contractor (e.g., The AGF structure may be a fixed percentage of the billed eligible revenue).
Audio Conference - A feature that allows a call to be established among three or more stations in such a manner that each of the stations are able to carry on a communication with all the other stations.
Audit Trail - A record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.
Authentication - Verification of the identity of a user, device, or other entity in an IT system, often as a prerequisite to allowing access to resources in a system.
Authorization Code - An assigned code provided by the user to gain access to pre-subscribed EIS contractor-provided services and features.
Authorized User - An organization or user that is authorized to use the EIS contract and/or associated systems, including all Federal Agencies, authorized Federal contractors, agency-sponsored universities and laboratories, and when authorized by law or regulation, state, local, and tribal governments, and other organizations. All organizations listed in General Services Administration (GSA) Order OGP 4800.2I (as updated) are also eligible.
Automatic Call Distributor (ACD) - The device used by many offices to distribute incoming calls among employees; answers calls, determines how to handle the call, alerts the caller to remain on the line and then transfers the call to the first available employee

Automatic Message Accounting (AMA) - An automatic system for recording data describing the origination time of day, dialed number and time duration of a call for purposes of billing.

Automatic Number Identification (ANI) - A service feature in which the directory number or equipment number of a calling station is obtained automatically.

Automatic Protection Switching (APS) - Switching architecture designed for SONET to perform error protection and network management from any point on the signal path.

Automatic Switched Optical Network (ASON) - A multi-client versatile intelligent platform that enables automatic management of signaling and routing through a network. Enables policy-driven control of an optical network. Goal is a type of bandwidth on demand (BoD). Usually refers to Wide Area Networks (WANs)

Availability - Availability is the ratio of the time during which a service is available to the user (e.g., to originate and terminate calls) to the total amount of time in the calendar month. Availability is expressed as a decimal between 0 and 1, and is normally calculated for one calendar month of service.

Availability of Service - Defined as "The percentage of time a given service is available." Calculate as:

$$Availability(\%) = \frac{ElapsedTime - OutageTime}{ElapsedTime} \times 100$$

B Channel - The International Telegraph and Telephone Consultative Committee (CCITT) designation for a clear channel, 64 kb/s service capability provided to a subscriber under the Integrated Services Digital Network offering. (See Integrated Services Digital Network)

Bandwidth - The difference, in hertz (Hz), between the highest and lowest frequencies of a transmission channel. Also used to identify the maximum amount of data that can be sent through a given transmission channel per second.

Bare Metal Virtualized Servers – Servers running on "bare metal" or high-speed standardized generic hardware and using open-source software, as opposed to traditional servers that use proprietary hardware and software. "Virtualized" refers to their ability to be configured by software to look like servers running different operating systems or multiple instances of operating systems for different clients. The control software for these virtualized servers is usually called a "hypervisor."

Basic Rate Interface (BRI) - An Integrated Services Digital Network (ISDN) multipurpose user's interface standard that denotes the capability of simultaneous voice and data services provided over 2B+D channels, two clear 64 kb/s channels (B channels) and one clear 16 kb/s channel (D channel) access arrangement to each subscriber's location as defined by International Telecommunications Union/Telecommunications Service Sector (ITU-TSS) I.412. (See B Channel and D Channel)

Best Commercial Practice - That method(s), process(es), procedure(s), system(s), and/or usage that is commonly implemented in the business world and that is generally agreed to have produced the most satisfactory or desirable result(s) on a consistent basis.

Bidirectional Line Switched Ring (BLSR) - A form of synchronous optical network (SONET) transmission that uses 2 rings for communication. The data flow on these two rings is opposite:

clockwise on one and counterclockwise on the other. The use of BLSR transmission allows half of the data communication devices to be served by one ring and half to be served by the other.
Bidirectional Path Switched Ring (BPSR) - SONET transport network configuration in which network nodes are connected in a ring and traffic can be instantly re-routed in the other direction around the ring in the event of a cable cut or degradation of optical signal, thereby routing around the point of failure.
Billed Price - Includes the actual price of equipment and/or services, AGF, and any billed charges that are defined in the EIS contract(s).
Billed Eligible Revenue - This represents revenue billed by the contractor that is included in the calculation of the Associated Government Fee (AGF) fee.
Billing Codes - These are specific alpha and/or numeric identifiers that are used in the contractor's commercial billing systems to represent various billing elements (e.g., feature charge type, transmission type, etc.).
Billing Dispute - A government notification to the contractor noting a difference between an actual invoiced amount and the correct amount, based on the contract.
Billing Inquiry - A question or issue in the area of billing which may lead to a billing dispute.
Billing Invoice – A contractor file produced not later than the 15th business day of every month containing all the chargeable elements of services delivered.
Billing Output files - This represents contractor output files related to contractual billing deliverables that are required by the government.
Bit - The smallest unit of data transmission, representing either a binary 1 or a 0.
Bit Error - An error in the transmission of a single bit.
Bit Error Rate (BER) - The number of bit errors divided by the total number of bits transmitted, received, or processed over some stipulated period.
Burst Size - The number of bytes that can be transmitted in a continuous stream.
Business Day - Any Monday through Friday that is not a US Federal holiday. *See also Government Business Day.*
Business Support System (BSS) - A system used to allow a network operator to perform the administrative portions of the business. These functions include billing, service ordering, customer support, service management, inventory management, and program management. For purposes of this RFP, the definition includes all systems required to support the communications company including billing, service ordering, customer support, service management, inventory management, and program management.
Busy Hour Grade of Service (GOS) - Busy hour GOS is a KPI for VS and is defined as the proportion of calls that cannot be completed during the customer's busy hour because of limits in the call handling capacity of one or more network elements (e.g., all trunks busy). For example, P.01

GOS indicates that one percent of the calls attempted are not being completed during the busy hour.
Byte - A set of eight bits that represents a single unit.
Call Detail Records (CDR) - Network record (voice, data, or other) that includes call or event details, such as type, time, duration, originator, and destination; CDR may apply to network monitoring, traffic accounting, and billing.
Case Description - Contains sufficient information to distinguish one case from another of the same CLIN. This description will be used by the government agencies to assist in evaluation.
Channel Service Unit / Data Service Unit (CSU/DSU) - Devices that combine the functionality of data service units (DSU) and channel service units (CSU) to adapt data from user communication systems to service provider communication lines with multiple channels.
Circuit - The complete transmission path between two endpoints over which one-way or two-way communication may be provided. A circuit may provide one or more channels.
Circuit Emulation Services (CES) - A service that transports TDM-based traffic over a Metro Ethernet Network and looks to the user like a TDM circuit such as a T1.
Circuit Switched Data Service (CSDS) - Provides a synchronous, full duplex, totally digital, circuit-switched service at multiple data rates, including integral multiples of DS0 data rates (i.e., NxDS0, where N = 1 to 24) to on-net and off-net locations.
Circuit Switched Voice Service (CSVS) - Supports voice calls, whether initiated from on-net locations or from off-net locations after verification of authorization code, to be connected to all on-net and off-net locations by direct station-to-station dialing throughout the United States.
Class of Service (COS) - Classification of packets (or other transmission unit) for the purpose of treating certain classes or flows of packets in a particular way compared to other packets. For example, some classes may be expedited. Usually defined by specific service KPIs.
Classmark - A designator used to describe the service feature privileges, restrictions, and circuit characteristics for lines or trunks that access a switch.
Clear Channel - In networking, a signal path that provides its full bandwidth for a user's service. *Note:* No control or signaling is performed on this path (e.g., 64 kb/s clear channel).
Cloud - Set of servers and computers in a large installation accessed over the Internet or a private network capable of storing user data and/or downloading data and applications to user devices. The cloud can also execute user programs and carry out other data processing functions.
Code Division Multiple Access (CDMA) - A system that allows multiple users to share one or more radio channels for service by adding a unique codes to each data signal being sent to and from each of the radio transceivers. These codes are used to spread the data signal to a bandwidth much wider than is necessary to transmit the data signal without the code.
Commercial Best Practice - Synonymous with "Best Commercial Practice"

Committed Burst Size (CBS) - The size up to which subscriber traffic is allowed to burst and still be in profile and not discarded.
Committed Information Rate (CIR) - A guaranteed minimum data transmission rate of service that will be available to the user through a network.
Common Language Location Identification Code (CLLI) - A location identification code that complies with American National Standard Institute (ANSI) standard T1.201-1987. The eight character mnemonic code is used to uniquely identify a location in the United States, Canada or other countries. These codes are known as CLLI or "Location Codes" and may be used in either a manual or mechanized record keeping system.
Compatibility - A property of systems that allows the exchange of necessary information directly and in usable form. *Note:* This implies use of identical or compatible protocols.
Competitive Local Exchange Carrier (CLEC) - A telephone service company that provides local telephone service that competes with the incumbent local exchange carrier (ILEC).
Computer Supported Telephony Applications (CSTA) - An interface created by ECMA to support computer telephony integration (CTI). ECMA is an industry association dedicated to the standardization of Information and Communication Technology (ICT) Systems.
Computer Telephony Integration (CTI) - CTI is the integration of computer processing systems with telephone technology.
Contract Line Item Number (CLIN) - A unique number used to identify billable items; a term used to describe an item that can have a single unit price; a contract line item must be identified separately from any other items or services on the contract.
CONUS - The 48 contiguous United States plus the District of Columbia.
Coordinated Universal Time (UTC) – A time standard commonly used across the world. .
Core Based Statistical Area (CBSA) - Metropolitan and Micropolitan geographic entities delineated by OMB for use in collecting, tabulating and publishing federal statistics (see OMB Bulletin No. 13-01, dated February 28, 2013).
Credit - An arrangement to reduce the amount owed by the customer on a future invoice by an agreed amount or for other Billing Adjustment (BA) reasons.
Critical Service Level - A level of service defined for government applications that specify higher levels of availability and performance than is assured by Routine Service.
Customer - Any entity included in OGP 4800.2I that purchases an EIS service or catalog item
Customer Network Management (CNM) - A data integration system that takes data from a service provider's fault, performance, and order management and provisioning systems, and integrates the data into a near real-time view for the enterprise customer.
Customer Network Management (CNM) Function - Provides an interface between users and the

contractor's administrative and operational data, allowing users on-line access to "read" and download user's data while ensuring the service providers maintain information security and control.
Customer Relationship Management (CRM) - A process or system that coordinates information that is sent and received between contractors and customers. CRM systems are used to order, bill, to schedule activities, allocate resources, and help control the sales activities within a company.
Customer Support Office (CSO) - An organization which will be established by the contractor to provide direct, day-to-day customer service to the government. Also referred to as Customer Service Center (CSC).
Customer Want Date (CWD) - This represents the data by which the agency/customer desires to have service installed.
Cutover - The physical changing of circuits or lines at a telecommunications location after completion of service installations by a contractor.
D Channel - In ISDN, the 16 kb/s segment of a 144 kb/s, full-duplex subscriber service channel that is subdivided into 2B+D channels, i.e., into two 64 kb/s clear channels (B Channel) and one 16 kb/s channel (D Channel) for the ISDN basic rate.
Dark Fiber - Deployed fiber optic cable or cable strand that is not being used to transmit light waves. It is installed, but is not yet operational or has been taken out of service.
Data Dictionary - A set of information describing the contents, format, and structure of a database and the relationship between its elements.
Data Encryption Standard (DES) - A cryptographic algorithm for the protection of unclassified computer data, issued as Federal Information Processing Standard Publication 46-1. Obsolete, replaced by Advanced Encryption Standard (AES).
Data Integrity - The property that data meets a predefined level of quality or acceptability.
Decibel (dB) - A measurement of power increase or decrease based on taking the logarithm of the ratio of the power level being measured to a standard power level.
Dedicated Service Types - The access and transport service types generally based on the use of fixed transmission media and generally billed on a monthly recurring basis.
Dense Wavelength Division Multiplexing (DWDM) **-** A fiber-optic transmission technique that employs many closely-spaced light wavelengths to transmit data. Each light wave transmits a different data stream. ITU grid spacing for wavelengths in DWDM systems is 0.8 nm but is technically defined in terms of frequency (100 GHz).
Dialed Number Identification Service (DNIS) - A call identification service typically provided by a toll free (800 number) network. The DNIS information can be used by the PBX or automatic call delivery (ACD) system to select the menu choices, call routing, and customer service representative information display based on the incoming telephone number.
Digital Signature - A quantity associated with a message or file, e.g., a message digest encrypted with a

private key, which only someone with access to a person's private key could have generated, but that can be verified through access and use of the associated public key. Usually considered as legally equivalent to a written signature.
Digital Subscriber Line (DSL) - A technology for transmission of digital information on a copper wire pair. Although the transmitted information is in digital form, the transmission medium is usually an analog carrier signal (or the combination of many analog carrier signals) that is modulated by the digital information signal.
Direct Billing - Agencies are invoiced directly by the contractor and pay the invoice directly to the contractor. The contractor is responsible for the collection of charges and AGF directly from the billed agencies or sub-agencies. GSA will not be responsible for any charges directly invoiced to any agency or sub-agency.
Direct Inward Dialing (DID) - Direct Inward Dialing (DID) connections are trunk-side (network side) end office connections. The network signaling on these 2-wire circuits is primarily limited to 1-way, incoming service. DID connections employ different supervision and address pulsing signals than dial lines. Typically, DID connections use a form of loop supervision called reverse battery, which is common for 1-way, trunk-side connections. Until recently, most DID trunks were equipped with either Dial Pulse (DP) or Dual Tone Multifrequency (DTMF) addresses pulsing.
Direct Ordering - A process in which agencies place orders directly with the contractor by using the contractor's ordering system or other processes agreed to by the parties
Direct-Billed Agency - A government agency or sub-agency that has elected to receive its billing directly from the contractor. Additionally, this represents a government agency or sub-agency that pays the contractor directly for services provided by the contractor.
Do Not Disturb (DND) - A term to describe a telephony feature that enables a user to temporarily block all calls to their telephone extension. DND provides the ability to temporarily block calls to a station number. The feature can be activated and de-activated by the subscriber. Outgoing calling capability is allowed when the DND state is activated. This capability can be administered on a station basis according to the subscribing agency's needs.
Domestic - Includes both CONUS and OCONUS regions
Dual-Tone Multifrequency Signaling - A telephone signaling method employing standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four relatively high frequencies.
Dynamic Allocation - A method for allocating charges among agencies in a shared tenant arrangement which applies to situations where the ANI is known for the agencies. *See Shared Tenant.*
E&M Signaling - In telephony, an arrangement that uses separate leads, called respectively the "E" lead and "M" lead, for signaling and supervisory purposes.
Effective Billing Date (EBD) - This represents the billing start date and may not precede the Service Order Completion Notice (SOCN) "complete date." Likewise, the billing end date must be the actual disconnect date indicated on the SOCN.
Electronic Access - The capability to access information via on-line access (dedicated or dial-up),

electronic mail, and facsimile.
EDI – Electronic Data Interchange
EINSTEIN – See National Cyber Protection System
Electronic Fund Transfer (EFT) - Any transfer of funds, other than a transaction originated by cash, check, or similar paper instrument, that is initiated through an electronic terminal, telephone, computer, or magnetic tape, for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit an account. The term includes Automated Clearing House transfers, Fedwire transfers, and transfers made at automatic teller machines and point-of-sale terminals. For purposes of compliance with 31 U.S.C. 3332 and implementing regulations at 31 CFR part 208, the term "electronic funds transfer" includes a government-wide commercial purchase card transaction.
Electronic Mail (e-Mail) - A process of sending messages in electronic form. These messages are usually in text form. However, they can also include images and video clips
Emergency Change - Represents a change to an invoice's content or format that is required to occur prior to the minimum 60-day frequency.
Enclave - In this RFP, refers to Security Enclaves. A set of information and processing capabilities that are protected as a group. The information processing capabilities may include networks, hosts, or applications.
Encrypt - To convert plain text into an unintelligible form by means of a crypto system.
End of Unacceptable Service Performance - The time following the start of a period of unacceptable service performance at which time all KPIs once again meet or exceed their associated AQLs.
End-to-End - Telecommunications service from the originating user's terminal to the destination user's terminal. As applied in this document, this term refers to Service Delivery Point (SDP) to SDP service.
Enhanced 911 (E911) - An emergency telephone calling system that provides an emergency dispatcher with the address and number of the telephone when a user initiates a call for help. The E911 system has the capability of indicating the contact information for the local police, fire, and ambulance services that are within a customer’s calling area.
Enterprise Infrastructure Solutions (EIS) - A comprehensive solution-based vehicle to address all aspects of federal agency information technology telecommunications, and infrastructure requirements.
Enterprise Infrastructure Solutions (EIS) Services - Services provided by the contractor to the customers under the EIS contract acquisition(s).
Envelope - In the context of message handling systems, as used in this document, envelope is an object that carries addressing information, and attributes (e.g., date, time, priority and subject) required for transporting the message.

Error Free Second (EFS) - A one second interval of digital signal transmission in which no transmission error occurs.
Errored Block - A data block in which one or more bits are in error.
Errored Second (ES) - A one-second interval of digital signal transmission in which at least one transmission error occurs.
Ethernet Private LAN (E-LAN) - A multi-point to multi-point service where disparate LAN segments are connected to form a single virtual LAN. Appropriate applications are inter and intra-city LAN connectivity, router interconnect and server consolidation. E-LAN can be offered over either a Metropolitan Area Network (MAN) or a Wide Area Network (WAN).
Ethernet Private Line (E-LINE) - A point-to-point service where bandwidth is reserved. E-LINE ES is useful for mission critical traffic. E-LINE resembles traditional Time Division Multiplexing (TDM) private line service. Appropriate applications are router interconnect, business continuity, and disaster recovery.
Exchange Rates - Shall be those in effect at close of business on the first working day of each billing period, as published by the Federal Reserve Statistical Release Foreign Exchange Rates Monthly Update or other mutually agreed source. No mark-ups or overhead charges shall be permitted on currency conversions.
Expedited Service Class A - The ordering agency requires priority provisioning for National Security / Emergency Preparedness (NS/EP) circumstances, or under circumstances in which the National Communications System (NCS) invokes the Telecommunications Service Priority (TSP) system. *See also Class A Expedited Implementation*
External Timing Reference (ETR) - Facilitates the synchronization of time-of-day (TOD) clocks to ensure consistent time stamp data in an installation with multiple, coupled systems.
Fail-Over Time - The time interval between the loss of a restorable network data link and its automatic restoration by imbedded management protocols.
Feature - An additional capability beyond basic service that is to be selected at the option of the user. Features are normally separately priced, although some features have been defined to be not separately priced.
Federal Acquisition Regulation (FAR) - The primary regulation for use by all Federal Executive Agencies in their acquisition of supplies and services with appropriated funds. It became effective April 1, 1984 and is issued within applicable laws under the joint authorities of the Administrator of General Services, the Secretary of Defense, and the Administrator for the National Aeronautics and Space Administration, under the broad policy guidelines of the Administrator, Office of Federal Procurement Policy, Office of Management and Budget.
Federal Agency - In FAR definition, means any executive agency or any independent establishment in the legislative or judicial branch of the government (except the Senate, the House of Representatives, the Architect of the Capitol, and any activities under the Architect's direction).
Federal Communications Commission (FCC) - Federal Agency established by the Communication Act of 1934 that oversees commercial spectrum usage, interstate telecommunications, and all international services originating and terminating in the United States.

Federal Information Security Management Act (FISMA) - a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107–347, 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States.[1] The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
Federal Relay Service - A Federal Government-provided service that acts as an intermediary between hearing individuals and individuals who are deaf, hard of hearing, or have speech disabilities.
Federal Telecommunications Recommendations (FTR) – A set of telecommunications recommendations for the design and procurement of telecommunications equipment/services for the National Communications System (NCS). The FTR are issued by the NCS technology and program division, after approval by the FTR standards committee and deputy manager, NCS, pursuant to Executive Order 12472, Public Law 104-113 and NCS directive 4-1. *{Source: NCS web page}*
Fiber Connectivity (FICON) - An IO protocol used between IBM (and compatible) mainframes and storage. It takes the higher layer ESCON protocol, analogous to SCSI, and maps into onto a Fiber Channel transport.
File Transfer Protocol (FTP) - A Transmission Control Protocol/Internet Protocol (TCP/IP) service that supports bidirectional transfer of binary and ASCII files without loss of data between local and remote computers on the Internet. The FTP command set allows a user to log onto a remote server over the network, list file directories and copy files.
FIPS 140-2 Encryption – a U.S. government computer security standard used to accredit cryptographic modules.
Firewall - A system that manages a boundary between two networks to control access between the networks. A firewall as a single point of entry to an organization's intranet from the Internet provides a method for the security official to limit public access to data on an organization's intranet while allowing users on the intranet to access the WWW.
Firm Order Commitment Date – The date that the contractor commits to provide the service in a state ready for the customer to use and the date that the government expects to accept the service and billing to become effective. It is the date specified on the Firm Order Commitment Notice in accordance with Section G.3.3 (Ordering Services).
Fraudulent Use of Services - Any use of EIS services for any functions or activities not authorized by the government.
Full-Duplex - A mode of operation in which simultaneous communication in both directions may occur between two terminals. Contrast with half duplex or simplex operation in which communications occur in only one direction at a time.
General Packet Radio Service (GPRS) - A portion of the GSM specification that allows packet radio service on the GSM system. The GPRS system adds (defines) new packet control channels and gateways to the GSM system.

Gigabit Ethernet (GigE) - Gigabit Ethernet (GE) is a data communication system that combines Ethernet technology with fiber optic cable transmission to provide data communication transmission at a Gigabit rate.
Gigabits per second (Gbps) – A measure of data transfer speed equal to one billion (10^9) bits per second.
Gigabyte (GB) – A measure of the size of binary data stored in memory or fixed media equal to 1,073,741,824 (2^{30}) bytes.
Gigahertz (GHz) - A measure of frequency equal to one billion (10^9) cycles per second. Signals operating above 1 GHz are commonly known as microwaves.
Government Data Elements - Data elements related to billing that are required by the government, and allows the government, at a minimum, to: • Verify information back to a service order, • Validate all charges, • Verify adjustments at the lowest level (e.g., service period of original charge type/description), • Enable the government to re-bill its own customers, • Assist with the management of inventory.
Government Fiscal Year – The 12-month period ending on 30 September of that year, having begun on 1 October of the previous calendar year
Government Furnished Equipment (GFE) - Property in the possession of, or directly acquired by the government and subsequently made available to the contractor. (See Government Furnished Property (GFP)
Government Furnished Property (GFP) - Property in the possession of, or directly acquired by the government and subsequently made available to the contractor.
Grade of Service (GOS) - A term associated with telecommunications service indicating the probability of a call being blocked during a call attempt during the busy hour, expressed as a decimal fraction.
Ground Start - A supervisory signal from a terminal to a switch in which one side of the line is temporarily grounded.
GSA Conexus - GSA's next-generation network solutions management system. This system is distinct from GSA Systems.
GSA Contracting Officer - The GSA contracting officer who administers EIS contracts.
GSA Systems - The set of tools used by GSA to manage the contract and TOs issued under the contract. These systems are distinct from GSA Conexus.
HyperText Markup Language (HTML) - Authoring software language used on the Internet and for creating WWW pages. HTML is essentially text with embedded HTML commands identified by angle brackets and known as HTML tags.

HyperText Transfer Protocol (HTTP) - The communications protocol used by a Web Browser to connect to Web servers on the Internet.
HyperText Transfer Protocol Secure (HTTPS) - The protocol for accessing a secure Web server. The use of HTTPS in the Uniform Resource Locator (URL) directs the message to a secure port address instead of the default Web port address of 80.
Identification (User ID) - The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.
Inbound - A switched connection made from a non-domestic location to a domestic location.
Indefeasible Rights of Use (IRU) - In telecommunications, Indefeasible Right of Use (IRU) is the effective long-term lease (temporary ownership) of a portion of the capacity of an international cable. This term is used in Dark Fiber Services.
Individual Case Basis (ICB) – Applies to a situation with special end-user requirements, for which special arrangements are made with the contractor where fixed pricing could not have been determined or could not apply.
Infrastructure as a Service (IaaS) – Cloud-based offering in which user gains access to virtual machines, servers, storage, and other infrastructure for the purpose of implementing a data center, for system testing, or other purpose. Users typically install their own images or operating systems on the cloud infrastructure.
Institute of Electrical and Electronics Engineers (IEEE) - An organization formed in 1963 that represents of electrical and electronics scientists and engineers.
Integrated Services Digital Network (ISDN) - A service that provides end-to-end digital connectivity to support a wide range of services, including voice and non-voice services, to which users have access by a limited set of standard multi-purpose user network interfaces, as defined in the ITU-TSS I series. (See basic rate interface and primary rate interface.)
Interactive Voice Response (IVR) - IVR is a process of automatically interacting with a caller through providing audio prompts to request information and store responses from the caller. The responses can be in the form of touch-tone(tm) key presses or voice responses. Voice responses are converted to digital information by voice recognition signal processing.
Interconnection - The linking together of interoperable systems.
Inter-exchange Carrier (IXC) - Also known as long distance carriers, inter-exchange carriers (IXCs) interconnect local systems with each other. For inter-exchange connection, networks as a rule connect to long distance networks through a separate toll center (tandem switch). In the United States, this toll center is called a point of presence (POP) connection.
Intermediate Reach – Single – Longitudinal Mode (IR1-SLM) - Intermediate Reach (IR) optical interfaces refer to optical sections with system loss budgets from 0 dB to 11 or 12 dB. Typically, low power SLM or MLM laser transmitters are used at the lower bit-rates, while high-power SLM lasers are used at the higher bit-rates.

International Telecommunications Union (ITU) – see "Consultative Committee for International Telephony And Telegraphy (CCITT)"
Internet - A worldwide interconnection of individual networks operated by government, industry, academia, and private parties.
Internetworking - The process of interconnecting a number of individual networks to provide a path from a terminal or a host on one network to a terminal or a host on another network. The networks involved may be of the same type, or they may be of different types. However, each network is distinct, with its own addresses, internal protocols, access methods, and administration.
Interoperability - The ability of systems to provide services to and accept services from other systems and to cause services from different systems to operate effectively together so as to achieve the throughput and service quality (i.e., required grade-of-service, transmission quality, and feature capability) that is agreed to be acceptable. The condition achieved among telecommunication systems when information or services can be exchanged directly and satisfactorily between them and/or their users. Interface devices or gateways may be placed between equipment or systems in order to achieve interoperability.
Inventory Reconciliation (IR) – Deliverable document that compares delivered service to ordered services and lists discrepancies.
Invoicing - The process of preparing and forwarding a list of charges to the government for services rendered by the contractor.
IP-Security (IPsec) – A group of IP security measures which together comprise a highly secure tunneling protocol for IP communications.
IS-41 – Intersystem Signaling, also known as ANSI-41. Mobile cellular telecommunications system standard to support networking of switches. Facilitates inter-switch operations such as call handoff and roaming authentication.
Jitter - Jitter, also known as cell delay variation or packet delay variation, is a measure of the variance of cell or packet transfer delay. High variation implies the need for larger buffering for delay-sensitive traffic such as voice and video. Jitter is caused by several factors that combine to cause packet delay variation, including variations in the propagation delay, queuing delays at various intermediate switches, and service times at switching points.
Key Performance Indicator (KPI) - A measurable service attribute that is critical to the proper functioning and delivery of a telecommunications service. KPI types are listed in Sec. C.1.8.3. Each EIS service is associated with KPIs that are specified in Section C.2 (Technical Requirements).
Kilobits per second (Kbps) – A measure of data transfer speed equal to one thousand (10^3) bits per second.
Kilobyte (KB) – A measure of the size of binary data stored in memory or fixed media equal to 1,024 (2^{10}) bytes.
Kilohertz (KHz) - A measure of frequency equal to one thousand (10^3) cycles per second.

Last Number Dialed (LND) – A term to describe a telephony feature that enables a telephone device to dial the most recently dialed telephone number.
Latency – Also known as cell latency, cell transfer delay, or packet transfer delay, it is the round-trip delay between transmission and receipt of a packet measured between network access points. Normally latency is expressed in milliseconds and the rate of delay is sampled over a brief period, typically one minute or less, to arrive at an average latency figure. Latency includes propagation delays, queuing delays at various intermediate components such as routers and switches, and service times at switching and routing points.
Layer 2 Tunneling Protocol (L2TP) - A protocol that is used to allow a secure communication path, a virtual private network link, between computers. It is an evolution of earlier point-to-point tunneling protocol (PTPP) as it offers more reliable operation and enhanced security. L2TP enables private communication lines through a public network. L2TP was developed via the Internet Engineering Task Force (IETF).
Layer 3 – The network layer in the Open Standards Interconnection Model (OSI). Layer 3 protocols handle routing within and between networks.
Link Capacity Adjustment Scheme (LCAS) - SONET term referring to a portion of the overhead in a SONET frame.
Local Area Network (LAN) - A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. .
Local Exchange Routing Guide (LERG) – A Telcordia publication that relates Numbering Plan Area (NPA)/NXX to the Vertical and Horizontal (V&H) and CLLI Code of the associated wire center.
Local Government Contact (LGC) – An individual designated by a CO on a service request to interface with the contractor at a specific agency location on his behalf. LGC participates in service transition planning and implementation activities for a location, however, the decision to change or modify a service order placed by the CO or COR, remains with the CO or COR.
Local Number Portability (LNP) - LNP is the process that allows a subscriber to keep their telephone number when they change service provider in their same geographic area. Local number portability requires that carriers release their control of one of their assigned telephone numbers so customers can transfer to a competitive provider without having to change their telephone number. LNP also involves providing access to databases of telephone numbers to competing companies that allow them to determine the destination of telephone calls delivered to a local service area.
Location – In this document, is a physical place where (1) a user of EIS services resides or (2) telecommunications services are available or (3) EIS services are delivered. Also construed to include wireless terminals. *(See Agency locations, SDP locations, PSTN locations)*
Long Haul (LH) – A communication system which includes a number of drop/add points, repeaters locations, over long distances that extend outside the local service area; a microwave system that the longest radio circuit of tandem radio paths exceeds 402 km (250 miles).
Loss - The amount of electrical attenuation in a circuit, or the power consumed in a circuit component.

Management Information Base (MIB) - In Simple Network Management Protocol (SNMP), the set of information about a managed object used by the management program.
Mandatory – These are services, features, or equipment which the contractor must propose. Any mandatory service, feature or equipment proposed must be priced.
Mapping - In Electronic Data Interchange (EDI), mapping refers to a defined process to translate a company's proprietary data layout to an interoperable EDI format.
Mean Opinion Score (MOS) - In voice communications, particularly Internet telephony, the mean opinion score (MOS) provides a numerical measure of the quality of human speech at the destination end of the circuit. The scheme uses subjective tests (opinionated scores) that are mathematically averaged to obtain a quantitative indicator of the system performance.
Meet-Me Conference - Allows stations to be connected in a conference by dialing one access code at a particular time.
Megabits per second (Mbps) – A measure of data transfer speed equal to one million (10^6) bits per second.
Megabyte (MB) – A measure of the size of binary data stored in memory or fixed media equal to 1,048,576 (2^{20}) bytes.
Megahertz (MHz) - A measure of frequency equal to one million (10^6) cycles per second.
Minimum Point of Penetration (MPOP) - An FCC defined location in a building/premises where an SDP is located normally.
Mobile Satellite Service (MSS) - A form of wireless service that employs satellites as part of the wireless infrastructure and is capable of serving very large geographic areas. The use of MSS may be appropriate for areas that are economically not viable for land based radio towers or to provide wide area group call (dispatch type) services**.**
Monthly Billing Informational Memorandum - A report provided by the contractor to the government which includes, but is not limited to, items that will explain changes in billing, changes to data formats, new services added to the billing, and issues pertaining to balancing charges.
Monthly Recurring Charge (MRC) - A fixed charge paid monthly
Multi-Line Key Telephone Systems - Telephone station equipment conforming to the Electronic Industries Association (EIA) standard RS-478, first published in July 1981.
Multimedia - Pertaining to the processing and integrated presentation of information in more than one form, e.g., video, voice, music, data.
Multi-Mode Fiber (MMF) – Optical fiber that is designed to carry multiple light rays or modes of light concurrently, each at a slightly different reflection angle within the optical fiber core, that is used for relatively short distances. Differs from Single Mode Fiber (SMF) because it has a larger core (usually 50 or 60 micrometers compared to 9 micrometers).

Multiprotocol Label Switching (MPLS) - A network routing protocol based on switching packets through a network by the use of tag labels, instead of routing them. Since switching is much faster than routing, this method can speed up network performance. .
National Agency Check - The computerized search of the National Crime Information Center computer network of various government (state, local, Federal, and tribal) agencies.
National Cyber Protection System (NCPS), also known as EINSTEIN – Deep packet inspection system designed to look for malware in packets traversing the Internet and destined for delivery to a government agency.
National Security and Emergency Preparedness Requirements (NS/EP) - Requirements for capabilities that maintain a state of readiness or respond to and manage an event or crisis (local, national, or international), which causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security and emergency preparedness posture of the U.S. EIS NS/EP requirements are consistent with guidance from the DHS Office of Emergency Communications.
National Telecommunications and Information Administration (NTIA) - A policy unit of the Department of Commerce which assigns frequencies in the spectrum used by the federal government. The NTIA also advises the President and Congress on telecommunications issues.
National Telecommunications Management Structure (NTMS) - NTMS is a principal Government Emergency Telecommunications Service (GETS) supported functions for providing network management during national emergency.
National Television Standards Committee (NTSC) Standard - The North American standard (525-line interlaced raster-scanned video) for the generation, transmission, and reception of analog television signals. Now largely obsolete because of new digital video standards such as High-Definition (HD) television.
Network Entry Point - A system that receives ANSI X12 Electronic Data Interchange transactions and transfers them to Value Added Networks. A Network Entry Point can provide services such as archival, date and time stamp, file transfer, and access to other networks such as the Internet.
Network Functions Virtualization (NFV) - the virtualization of network equipment functions, which typically run on dedicated appliances, to now run on industry-standard servers, switches and storage devices with the aim of lowering costs, improving efficiency and increasing agility.
Network Site Code (NSC) - Identifies a physical location, a customer agency building, Physical Concentration Location, and/or Point of Presence. See Section B.4.1 for details.
Node - Center for the interconnection of two or more branches of a telecommunications network.
Non-Domestic - The worldwide countries and locations other than those defined herein as domestic.
Non-recurring Charge (NRC) - A cost for a facility, service, or product that only occurs one time or is not periodically charged.
North American Numbering Plan (NANP) – The numbering system that creates unique phone numbers for network dialing in the US, Canada, and some Caribbean islands; a numbering plan which

allows all stations conforming to the 10-digit dialing pattern of the Public Switched Network (PSN) to be accessed. The pattern is of the form NPA-NXX-XXXX where NPA= (Area Code); N = 2-9; P = 0-9; A = 0-9; and X = 0-9. The NANP is a subset of and consistent in format with the ITU/TSS ISDN E.164 Uniform numbering and addressing plan used worldwide.
North American Standard for Wireless Telecommunications Network Signaling (IS-41) – See "Intersystem Signaling 41 (IS-41)"
Not Separately Priced (NSP) - A capability or feature that is included in the price of the basic service.
Notification of Data File Loading Problems - An email notification provided by the GSA to the contractor intended to alert the contractor of system file loading problems associated with the media or data the contractor provided.
Numbering Plan Area (NPA) – The first three digits of a North American telephone number, often called an area code, in which the first digit cannot be a 1 or a 0 and that the remaining numbers can be 2 through 9.
OCONUS - U.S. territories and possessions outside of the contiguous 48 states. It includes Alaska, Hawaii, Guam, Puerto Rico, US Virgin Islands, Marshall Islands, Midway Island, Palau, Wake Island, American Samoa, Commonwealth of Northern Marianas Islands (CNMI) and Micronesia
Office of Emergency Communication (OEC) – The mission of the OEC is to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget in (1) the exercise of the telecommunications functions and responsibilities, and (2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack & recovery and reconstitution. {source *www.NCS.gov* website}. Formerly known as the National Communications System.
Official List Price (OLP) - Term defined under EIS to include a variety of possible list price types. For example, if the catalog item is equipment not manufactured by the contractor, the OLP could be the Original Equipment Manufacturer's Published List Price. When the catalog item is a service provided by the contractor, the OLP could be the contractor's Published List Price for the service.
Official Manufacturer's List Price – The manufacturer's list price for a SRE as found on an up-to-date document containing undiscounted list price information that is provided to a lessor or reseller of the SRE by the manufacturer, and that can be confirmed by similar documents provided by the manufacturer to other equipment or service providers or is available on its website.
Off-Net Call - A call between two or more stations, at least one of which is a presubscribed user or service delivery point (usually a PBX or Centrex) and at least one of which is not.
Off-Net Location – A location that is not presubscribed to services provided by EIS, i.e., a location "off" of the EIS network. Certain EIS services can transmit and receive communications with locations not "on" the EIS network, such as commercial telephone lines on the PSTN and personal computers connected to the Internet.
On-Net Call - A call between two or more on-net locations.
On-Net Location - A location that is presubscribed to services provided by an EIS contractor, i.e., a location "on" the contractor's EIS network. On-net locations may be implemented using either

dedicated access or a presubscribed switched access arrangement. On-net locations shall be construed to include presubscribed terrestrial and satellite service-based wireless handsets or terminals.
Optical Add-Drop Multiplexer (OADM) – A network element that allows the extraction/insertion of one or more wavelengths from/to the multi-wavelength signal as it is passed through the element.
Optical Carrier Hierarchy Level-N (OC-n) – In SONET systems, Optical carrier (OC-n) transmission is a hierarchy of optical communication channels and lines that range from 51 Mbps to 40 Gbps . The "n" is an integer (typically 1, 3, 12, 48, 192, or 768) representing the data rate.
Optical Transport Network (OTN) – Replacement for SONET that will do SONET functions such a framing in a manner more suited to faster provisioning and network flexibility. Designed to interface between Wave Division Multiplexing (WDM) equipment and higher layers in OSI protocol stack. Consists of six layers, of which Optical Transport Unit (OTU) and Optical Channel (OCh) are most commonly referred to.
Optical Wavelength Service (OWS) - Provides connectivity to data centers, carrier hotels, and enterprise businesses and tremendous bandwidth capacity of a dedicated wavelength connection, without the significant upfront capital costs or the management and maintenance issues associated with a dark fiber network.
Optional – Those services, features, or equipment which contractors may propose but are not required to propose. Any service, feature or equipment proposed must be priced.
Optronics – The combination of optical and electronic functions in one piece of telecommunications equipment that provide an interface between electrical and optical telecommunications modes.
Outage - A telecommunication service condition wherein a user is deprived of service due to a malfunction of the contractor's communication system.
Outbound - A switched connection made from a domestic location to a non-domestic location.
Password - A word, character, or combination of characters that permits access to otherwise inaccessible data, information, or facilities. Also referred to in this document as an authorization code.
Past Performance Information Retrieval System (PPIRS) - A database retrieval system utilized by the Contracting Officer (and Ordering Contracting Officer) in assessing past performance of contractors. In conformance with the government's need to record and maintain information on contractor performance during the life of this contract, the government periodically evaluates the manner in which the contractor performed in accordance with contract requirements such as: quality of service; cost efficiencies; timeliness; business relations; history of reasonable and cooperative behavior; commitment to customer satisfaction; and key personnel.
Payload - In a set of data, such as a data field, block, or stream, being processed or transported, the part that represents user information and user overhead information, and may include user-requested additional information, such as network management and accounting information. Note: The payload does not include system overhead information for the processing or transportation system.

Performance-based Contracting – In FAR definition, means structuring all aspects of an acquisition around the purpose of the work to be performed with the contract requirements set forth in clear, specific, and objective terms with measurable outcomes as opposed to either the manner by which the work is to be performed or broad and imprecise statements of work.
Period of Unacceptable Service Performance - Period of time during which the service provided is incapable of supporting one or more of the customer's uses or applications that normally would be supported by the service. The start and end of a period of unacceptable service performance may be reported either by the contractor or by the customer. *See Unacceptable Service Performance.*
Platform as a Service (PaaS) – Cloud-based offering in which providers deliver a computing platform, usually including operating system, programming-language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. In some cases resources are scaled automatically in response to user needs.
PMM (Price Management Mechanism) Demand Set - A statistically significant traffic set extracted from the contractor's EIS usage for each of the services subject to the PMM process and for the contract period under review by the PMM process.
Physical Concentration Location (PCL) - Any place where connections are aggregated. See Section B.4.1 for details.
Point of Presence (POP) – A contractor-owned or controlled physical location where network facilities provide EIS services and where user agency locations are connected to the network. See Section B.4.1 for details.
Polarization Mode Dispersion (PMD) - In single mode fiber optic cable, refers to the fact that the two orthogonal polarizations of light waves in the core travel at slightly different speeds, leading to slow smearing of pulses as they traverse the fiber. PMD can limit the highest bit rate that is achievable in a fiber optic system.
Post Office Protocol Version 3 (POP3) –Post Office Protocol version 3. A protocol used to retrieve e-mail from an e-mail server. POP3 is described in detail in IETF RFC 1939.
Preset Conference - A feature that allows designated users to establish a conference by dialing a single number.
Price Management Mechanism (PMM) - A special contract requirement establishing a process to ensure that EIS service prices remain competitive with prices paid by other large users of telecommunications services. The competitiveness of EIS service prices is examined by comparing the cost when EIS prices are applied to demand sets with the cost when pricing from comparison commercial and other government contracts, price schedules, and tariffs are applied to the same demand set. Reductions in EIS contractor prices will be required if a lower comparison cost is found through the PMM process.
Pricing Hub (PHub) - Used to assign a unique identifier to locations with the same price for the same access service type. See Section B.4.1 for details.
Primary Inter-exchange Carrier (PIC) - Refers to the company that is selected by the subscriber to be

its main long distance company. It is the carrier chosen by a subscriber to be accessible via simplified dialing pattern.
Primary Rate Interface (PRI) - An ISDN interface standard that is designated in North America as having a 23B+D channels. (See Integrated Services Digital Network)
Prime Contract - A contract or contractual action entered into by the U.S. for the purpose of obtaining supplies, materials, equipment, or services of any kind.
Prime Contractor - A corporation, partnership, business association of any kind, trust, joint-stock company, or an individual who has entered into a prime contract with the U.S.
Private Branch Exchange (PBX) - Telephone switching equipment designed to allow a large number of telephones in an office to call each other, and share one or more outside lines to connect to the PSTN. Conforms to the EIA standards RS-464 and RS-464-1, published in December 1977 and August 1982, and meeting Federal Communications Commission (FCC) registration requirements for interconnection to the public switched network.
Private Line Service (PLS) - The service category covering provision of private-line transmission of voice or data using end-to-end transmission media. (See Dedicated Transmission Service)
Program Management Office (PMO) - An office within the GSA/FAS organization responsible for management and contract administration of a telecommunications program. Within the context of this document, it refers to the specific PMO responsible for the EIS program.
Project – A project requires special treatment by the contractor due to the size, complexity, or importance of the services ordered as a project. The customer may request that the order be implemented as a project. In such cases, the contractor shall develop a Task Order Project Plan. Provisioning intervals will be as agreed to between the contractor and the ordering agency.
Project Identifier - A Project Identifier is a code or number assigned by the contractor or government and shown by the contractor on a series of service orders to identify each service order that is part of a larger group in progress.
Project Service Request - Multiple requests for service that are associated with a particular project and are related in such a manner that they should be implemented in a coordinated fashion.
Prompt Payment Clock - This represents the date and time, or the period of time from which the government has received all monthly billing deliverables as required by the contract until the payment has been made by the government to the contractor. GSA will start the Prompt Payment clock according to FAR Clause 52.232-25 when the detail billing has been delivered to the government (See Section G.4 Billing).
Public Safety Answering Point (PSAP) – A physical location where 911 emergency telephone calls are received and then routed to the proper emergency service.
Public Switched Telephone Network (PSTN) – Common domestic telecommunications network that interconnects private branch exchange trunks, telephones, Centrex systems, and wireless terminals and handsets.
Quality of Service (QoS) – User's experience over a network connection. Usually measured by a

defined set of engineering values for a service that is guaranteed by the contractor Typical QoS parameters are bandwidth, delay or latency, jitter, packet loss, and out-of-order delivery.
Radio Frequency (RF) - Those frequencies of the electromagnetic spectrum normally associated with radio wave propagation. RF sometimes is defined as transmission at any frequency at which coherent electromagnetic energy radiation is possible, usually above 150kHz.
Relay Service – *See Federal Relay Service*
Role Based Access Control (RBAC) – Allows only authorized users with appropriate permissions access to the BSS.
Routine Order – An order for which the contractor's standard provisioning interval applies.
Routine Service Level – A level of service that applies for most government applications and is expected to reflect commercial best practices for service availability and performance.
Satellite Internet Service (SIS) – Provides Internet access through satellite communications. This is mostly applicable to small rural sites without broadband wireline or wireless access or that need a backup Internet connection, and sites that require backup communications during a national emergency or disaster.
Sawtooth Effect – In this RFP, the effect observed when using declining unit prices in a set of increasing dollar ranges to determine a cost associated with a particular range. The cost is determined such that the last cost within a lower dollar range is higher than the first cost within the next higher dollar range, and the first cost within the next dollar range is lower than the last cost within the previous dollar range.
SDP Locations – *See Service Delivery Point (SDP)*
Secured E-Mail - Process by which electronic documents, reports, or files are provided or delivered to the government via E-Mail in a secured manner (e.g., E-Mail over a private network, encrypted E-Mail, encrypted attachment in an E-Mail).
Secured FTP Media - Distribution media by which electronic documents, reports, or files are provided or delivered to the government via File Transfer Protocol (FTP) server in a secured manner (e.g., SFTP, FTP over a Virtual Private Network, and FTP over a private network).
Secured Web-based Media - Distribution media by which electronic documents, reports, or files are provided or delivered to the government via a HTTP server in a secured manner (e.g., HTTPS, HTTP over a Virtual Private Network, and HTTP over a private network).
Security Violation - Any unauthorized action taken by any domestic or international party (contractor employee or non-employee) that: a) violates contractor's security policies, b) bypasses contractor's security mechanisms, C) gains unauthorized access to contractor's facilities, information, information systems, or management systems, d) intentionally affects the quality, integrity, or availability of services offered to the government, e) alters or destroys any EIS services information held by the contractor and/or provided to the government, f) discloses confidential or secret information, and/or g) compromises national security.
Service - The term "Service" refers to the primary unit of EIS technical and pricing requirements. It

includes all components and functions provided by the contractor to deliver a specific service, including the contractor's network, contractor-provided access arrangements and service related equipment. Individual services are grouped into "Service Types." *Also see "Service Types"*
Service Access Code (SAC) - The 3-digit codes in the NPA (N 0/1 X) format which are used as the first three digits of a 10-digit address in a North American Numbering Plan dialing sequence. Although NPA codes are normally used for the purpose of identifying specific geographical areas, certain of these NPA codes have been allocated to identifying generic services or to provide access capability, and these are known as SACs. The common trait, which is in contrast to an NPA code, is that SACs are non-geographic.
Service Delivery – A process which begins at the time an order is accepted by the contractor and ends at the time service is accepted by the customer. Service delivery includes service provisioning and service acceptance sub-processes.
Service Delivery Point (SDP) - the interface point at which a service is delivered by the contractor to the government or its designated agent. The SDP is the interface point for the physical or logical delivery of a service, the point at which performance parameters are measured to determine compliance with the contract, and the point used by the contractor to identify the pricing for services rendered.
Service Level Agreement (SLA) - An agreement between the government and the contractor to provide a service at a performance level that meets or exceeds the specified performance objective(s). The contract has specific KPIs for nearly all services. If a contractor does offer a service, it must comply with those KPIs. For each KPI, the contractor shall meet specified Acceptable Quality Levels (AQLs). Certain services are deemed sufficiently essential to government operations to also require mandatory Service Level Agreements (SLAs). If the specified service levels are not met, then the contractor shall issue specified credits.
Service Level Agreement Credit Request (SLACR) – Request for credit submitted to a vendor when one of the vendor's services has failed to meet the performance criteria specified in the associated Service Level Agreement.
Service Related Equipment (SRE) – Contractor-provided equipment (composed of one or more devices) used to meet the User to Network Interface (UNI) requirements for an individual service and/or to implement access aggregation and integration to provide a lower service delivery cost to the government. SRE is also contractor-provided equipment used to enable the requirements associated with the Management and Applications Services and Security Services. In this RFP, SRE will be offered only as needed to provide delivery of a service procured under an EIS contract.
Service Order - The documentation that contains all information required to obtain a service. Service orders can be placed against a TO. The service order functional requirements and ordering procedures include the submission of service orders by agencies and the receipt of notifications from the contractor at appropriate points in the ordering interval, service delivery and fulfillment process.
Service Order Acknowledgement (SOA) - The acknowledgement provided by a service provider (contractor) that an order has been received from the ordering agency.
Service Order Completion Notice (SOCN) - The notice that contains data elements notifying the agency that the service for a given order has been fully installed and is ready for acceptance.

Service Order Confirmation (SOC) - The notice a contractor provides the agency that contains the data elements that a service for a given order is accepted as a valid service with all the information needed to start service provisioning.

Service Outage – Either a complete loss of service or degradation of service that is so severe that it is not able to support a customer application. A service outage that is reported to the contractor as an out of service (OOS) condition must be documented by a trouble ticket. Any service outage automatically causes unacceptable service performance, as defined below.

Service Restoration – The point in time at which the contractor returns service to a condition in which all KPIs meet or exceed their associated AQLs following the opening of a trouble ticket for either unacceptable service performance or for a service outage.

Service Restoration Time – The interval of time between the opening of a trouble ticket for either a service outage or for unacceptable service performance and service restoration.

Service Type – Describe a group of individual services that are similar and are grouped to simplify specification, offering and evaluation processes. Within each Service Type, individual services are specified. In EIS, there are twelve (12) Service Types as follows:

1. *Data Service*. Includes services such as VPNS, Ethernet, Optical Wavelength Service, Private Line, SONET, Dark Fiber and Internet Protocol Service
2. *Voice Service*. Includes services such as IPVS, CSVS, Toll Free and CSDS.
3. *Contact Center Service*.
4. *Colocated Hosting Service*.
5. *Cloud Service*. Includes services such as Infrastructure as a Service, Platform as a Service, Software as a Service, Content Delivery Network Services.
6. *Wireless Service*
7. *Commercial Satellite Service*
8. *Managed Services*. Includes services such as Managed Network Service, Web Conferencing Service, Unified Communication Service, Integrated Performance Monitoring Service, MTIPS, Managed Security Services, Managed Mobility Service, Audio Conferencing, Video Teleconferencing and Intrusion Prevention Security Service.
9. *Access Arrangements*
10. *Service Related Equipment*
11. *Service Related Labor*
12. *Cable and Wiring*

Serving Wire Center (SWC) – The wire center (also called a central office) from which the user agency's premises would normally obtain dial tone from its Local Exchange Carrier; the wire center from which dial tone service is provided to a local exchange service customer.

Session Initiation Protocol (SIP) - In VoIP systems, a protocol used for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging over Internet Protocol (IP) networks.

Severely Error Second (SES) – A one second interval of digital signal transmission in which 30% or more of the data stream contains errors. The occurrence of 10 or more contiguous severely error seconds on a Private Line Service data circuit causes service unavailability.

Simplex Operation - That mode of operation in which communication between two points occurs in only

one direction at a time. Contrast with half duplex or duplex operation.
Single-Mode Fiber (SMF) – Optical fiber that is designed for the transmission of a single ray or mode of light as a carrier and is used for long-distance signal transmission. Has a smaller core than multi-mode fiber (9 micrometers vs 50 or 60 micrometers).
Software as a Service – Cloud-based offering in which providers manage infrastructure and platforms that run user-facing applications. Users access the applications from clients, often web-based clients. Applications may maintain user account information and store user data in the cloud. Typical examples include e-mail and banking.
Software Defined Networking (SDN) -An approach to networking in which control is decoupled from the physical infrastructure, allowing network administrators to manage a network fabric across multi-vendor equipment by use of control planes and virtualization.
Specification - A document that clearly and accurately describes the essential technical requirements for items, materials, or services, including performance requirements.
Standard Features - Capabilities included with a service that are not separately priced (NSP) and are typically not separately identified. If a standard feature is identified by a separate CLIN, its price shall be zero. Standard features are service dependent.
Start of Unacceptable Service Performance – The time at which any of the KPIs for the service begins to fail to meet its associated AQL. This may be documented from the contractor's monthly performance report or from a trouble ticket initiated by the customer or the contractor.
Sub-Agency - A subsidiary billing entity as defined by the parent agency and identified by an Agency Hierarchy Code.
Synchronous Digital Hierarchy (SDH) - The International Telecommunications Union standard for fiber optic synchronous transmission rates which begins at 155 Mbps. SONET is a subset of SDH, and for most applications is functionally the same at OC-3 and higher rates.
Synchronous Optical Network Services (SONET) – Layer 2 technology for transmitting digital data over optical fiber with high reliability and low error rates. Subset of SDH.
Tariff – Document filed by a regulated telephone company with a state public utility commission or the Federal Communications Commission. The tariff is a public document that details services, equipment and pricing offered by the telephone company to all potential customers.
Task Order- An order for services that contains all of the information required in FAR 16.505.
Telecommunications Device for the Deaf/Teletypewriter (TDD/TTY) - A device that permits individuals with speech and/or hearing impairments to make and receive telephone calls without assistance from others. A TDD or TDD-compatible device will be used by the speech/hearing-impaired user community to access the Federal Relay Service. A TDD generally consists of a keyboard, display screen, and a means (via modem or direct connection) to access a telecommunications network. It is recognized that this function can be performed by a computer with software enhancements. The term TTY may also be used in referring to this type of device.
Telecommunications Services - The services and solutions that deliver or augment communications

between users. It refers to a communications service or solution specified as a discrete offering or set of capabilities.
Telecommunications Service Priority (TSP) - The TSP program provides a framework for telecommunications services vendors to initiate, restore, or otherwise act on a priority basis to ensure effective NS/EP telecommunications services during national emergency. The TSP System applies to common carriers, to government, and to private systems that interconnect with commercially provided services or facilities.
Terabyte (TB) – A measure of the size of binary data stored in memory or fixed media equal to 1,099,511,627,776 (2^{40}) bytes.
Time to Restore (TTR) - The Time to Restore (TTR) SLA measures contractor performance on a per-incident basis. The contractor shall calculate the TTR using the following method: 1. Find the elapsed time between the time a service outage is recorded in the trouble ticketing system and the time the service is restored. 2. Subtract time for any scheduled network configuration change or planned maintenance. 3. Subtract time, as agreed to by the government, that the service restoration of the service cannot be worked on due to government-caused delays. Examples of government-caused delays include: a) The customer was not available to allow the contractor to access the Service Delivery Point or other customer-controlled space or interface; b) The customer failed to inform the contractor that a security clearance was required to access the SDP or customer-controlled space; or c) The government required service at a remote site and agreed that a longer transit time was required.
Transfer "off" - The transfer of service from the contract to a follow-on contract or service arrangement, managed by GSA in a coordinated way to prepare for the expiration of the contract.
Transfer "on" - The transfer of service from an EIS contract or a GSA local services agreement (LSA) to the contract
Traffic Model - A representation of traffic. A model of 5-year estimated traffic to be used in preparation and evaluation of the EIS price proposals.
Transition - The process for the coordinated transfer of service from a specified GSA incumbent contractor to a new EIS contractor.
Transport - The facility-based service arrangements that provide service specific connections between the contractors' POPs.
Trouble Ticket – The method used by the contractor to record a service trouble either detected by the contractor or reported by the customer to the contractor. It is the primary method used by the government and the contractor to report and track a service outage or for unacceptable service performance.
Unacceptable Service Performance – A period during which the service provided is not capable of properly supporting the customer's intended application or use. Unacceptable service

performance is caused by the failure of any combination of the key performance indicators (KPIs) to meet their specified acceptable quality levels (AQLs). Unacceptable service performance may or may not result in a service outage depending on the severity of service degradation; i.e., the amount by which the KPIs fail to meet their AQLs.
Uninterruptible Power Supplies (UPS) - An Uninterruptible Power Supply is a device that sits between a power supply (e.g. a wall outlet) and a device (e.g. a computer) to prevent undesired features of the power source (outages, sags, surges, bad harmonics, etc.) from adversely affecting the performance of the device.
Unique Billing Identifier (UBI) – The Unique Billing Identifier (UBI) is a contractor-assigned code that uniquely identifies a group of services that are related for ordering, billing and inventory purposes as well as uniquely identifying each component within that grouping.
User - An individual or agency that utilizes EIS services. *Also see Authorized User.*
User-to-Network Interface (UNI) – The specification of the physical, electrical, and signaling/protocol interface at the SDP for a specific information payload bandwidth or data transfer rate for interconnection of user equipment to an access segment.
Vertical and Horizontal (V&H) - Vertical and Horizontal coordinates result from a complex algorithm that projects the curvature of the earth onto a flat plane. These coordinates have been used in telephony since the late 1950's as a means to determine "airline" distance between two points via a simple formula. The projection algorithm uses latitude and longitude as well as various other factors in deriving V&H values. V&H's are used to identify locations and hence relative distances between network elements (e.g. switch locations), and between "rate centers" (e.g. the "center" of a rate exchange area). Such computations are necessary in cases where rates and costs for services are based on distance sensitive factors.
Very Early Smoke Detection Apparatus (VESDA) - A highly sensitive aspirating smoke detector installed in a data center is linked to the building management system which is monitored continually from a network operations centre, providing very early detection to help avoid fire, loss and business disruption. This is coupled with a gas based fire retardant that is environmentally friendly to put out fires instantly without damaging equipment.
Virtual Private Network (VPN) - Secure private communication path(s) through one or more non-private data networks that function as dedicated links between those points. To the users a VPN looks like a private network made up of dedicated links such as T1 or T3 lines. VPN connections allow data to safely and privately pass over public networks (such as the Internet).The data traveling between two points is encrypted for privacy.
Voice over Internet Protocol (VoIP) - A combination of technology and Internet protocols that allow the transmission of real-time voice communications across a data network.
Wavelength Division Multiplexing (WDM) - A method of transmitting several distinct communication channels through a single optical fiber via the use of a distinct separate infrared wavelength (optical frequency or "color") for each communication channel. Each such channel may be further subdivided into several logical channels via time division multiplexing or other methods**.**
Web Browser - Client software for connecting to and viewing documents on the WWW. A browser interprets HTML documents and displays them.

Web Browser/Server (WBS) - A Web Browser, a Web Server and their intended interaction. Web Browsers and Servers may communicate over the Internet and/or intranets.
Web Server - A Web site including hardware and software that includes the operating system, Web software, other software and data, or the software that manages Web functions at a Web site and makes web pages available to users.
Web Site - A computer on the Internet or an intranet running a Web Server that responds to HTTP and HTTPS request from Web Browsers.
Web-based - *See Web-based Media.*
Web-based Media - Distribution media by which electronic documents, reports, or files are provided or delivered to the government via a Hyper-Text Transmission Protocol (HTTP) server over the Internet.
Wide Area Network (WAN) - A communications network serving geographically separate areas. A WAN can be established by linking together two or more metropolitan area networks, which enables data terminals in one city to access data resources in another city or country.
Wire Center – The location of one or more local switching systems; a point at which customer loops converge.
Wire Center Serving Area – The area of an authorized telephone company's Local Exchange Service local calling area served by a single wire center.
Wireless - A categorization of switched and non-switched service types that generally use radio (e.g., mobile, cellular, or satellite radio) as their primary transmission medium. Generally excludes point-to-point terrestrial microwave.
Wireless Priority Service (WPS) - Wireless Priority Service (WP) allows authorized National Security and Emergency Preparedness personnel to gain priority access to wireless networks to initiate calls during an emergency when channels are congested.
Wireline - A categorization of switched and non-switched service types that generally use metallic cable, optical fiber cable, and point-to-point terrestrial microwave radio as their primary transmission media.
World Wide Web (WWW) - An Internet function for sharing of documents with text and graphic content that links documents locally and remotely.

J.13 List of Links

This section lists selected URLs referred to in this RFP.

J.13.1 Contracts/Federal Mandates/Executive Orders

FAR: https://www.acquisition.gov/?q=browsefar Clinger Cohen: https://www.fismacenter.com/Clinger%20Cohen.pdf

Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

Past Performance Information Retrieval System (PPIRS): http://www.ppirs.gov/

OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies: http://www.whitehouse.gov/omb/memoranda_2004

Electronic Product Environmental Assessment Tool (EPEAT):

https://www.epa.gov/greenerproducts/electronic-product-environmental-assessment-tool-epeat GETS Service:

- http://www.dhs.gov/government-emergency-telecommunications-service-gets

Wireless Priority Service (WPS):

- https://www.dhs.gov/wireless-priority-service-wps

Bureau of Labor Statistics (BLS) Department of Labor Employment and Training Administration's Occupational Information Network (O*NET):

http://www.onetonline.org/ BLS indices:

- Employment Cost Index (ECI): http://www.bls.gov/news.release/eci.toc.htm
- Producer Price Index (PPI): http://www.bls.gov/ppi/

J.13.2 Security

FIPS and NIST 800 Series: http://csrc.nist.gov/publications/index.html

FISMA: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

FedRAMP: http://www.FedRAMP.gov

- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and contractors," August 27, 2004; available at: http://www.idmanagement.gov/.

J.13.3 GSA

Network Services Program: http://www.gsa.gov/portal/category/22151

Core Based Statistical Areas (CBSAs):

- http://www.census.gov/geo/reference/gtc/gtc_cbsa.html
- http://www.whitehouse.gov/sites/default/files/omb/bulletins/2013/b-13-01.pdf

J.14 Form DD254


GSA FAS ITS EIS Top Secret Form DD254 0

J.15 Calculation of Economically Adjusted Prices (EAP)


EPA V.2.1.xlsx

J.16 Instructions for Gaining Access to AcquServe

J.16.1 AcquServe Access Guide for EIS (FEB 2015)


AcquServe Access Guide for EIS Feb 201

J.16.2 Agreement to Protect Sensitive Information


Agreement to Protect Sensitive Infc

J.16.3 EIS Offeror Application


EIS Offeror Application.doc

J.16.4 List of Designated Users


List of Designated Users.doc

J.17 AcquServe User Instructions

Refer to AcquServe, https://acquserve.eis.noblis.org for current version of User Guide.

J.18 DARS and DFARS Clauses

EIS DARS and DFARS Clauses.docx

J.19 Submission Matrix

Submission Matrix J.19 Amendment 12.›

J.20 Small Business Subcontracting Plan Outline (Model)

Section J Subcontracting Plan A

APPENDIX A

Submission Numbering Scheme

Contractors shall use the submission numbering scheme presented in this document. Contractors shall be responsible for assigning and maintaining submission numbers, and do not have to contact the government in order to generate a submission number. This scheme allows a single submission number to be used for several contractor submissions to the government that lead to a single contractor modification. The format of the complete scheme for coding submission numbers is as follows:

CCSSSSS.VVT, where:

			Type of Proposed Submission (T, alpha)
		Version Number (VV, numeric)	
	Submission Number (SSSSS, numeric)		

Contractor ID (CC, alphanumeric), as assigned by the government to indicate contractor.

Types of proposed submissions (“T”) include the following:

- “a” is any modification to the contract
- “c” is a catalog submission
- “t” is a TO-specific submission

Submission numbers (“SSSSS”) shall be five digits and shall be unique for each submission.

The version number (“VV”) is a two-digit version control number that begins with the value “01” and increases by 01 for each subsequent version. Using version numbers after the submission number allows for all correspondence generated for a single proposed contract modification, catalog submission, or TO-specific submission to have the same submission number.

The following examples demonstrate the proper use of the submission numbering scheme:

Example one: Company AA submits a proposed enhancement that requires four iterations to become a contract modification. The submission numbers are as follows:

AA00101.01a -> initial submission

AA00101.02a

AA00101.03a

AA00101.04a -> final submission that is accepted as a contract modification

Example two: Company BB submits a proposed price reduction that requires four iterations to become a contract modification. The submission numbers are as follows:

BB00101.01a -> initial submission

BB00101.02a

BB00101.03a

BB00101.04a -> final submission that is accepted as a contract modification

Note: It is the government's intent to keep and maintain logs of contract modification, catalog submission, and TO-specific submission activity using this submission numbering scheme.

MODIFICATION NUMBERING SCHEME

The modification number will consist of one alphabetical identifier followed by five alphanumerical identifiers, for example:

P: Issued by the Procuring Contracting Office (P00001)

A: Issued by the Administrative Contracting Office (A00001)

APPENDIX B

Example

The Submission Cover Letter for Contract Modifications must provide summary information as applicable.

The following files are included in this submission:

Submission Number	Technical (Volume I) Change Section	Management (Volume II) Change Section	Business (Volume III)	Price (Volume IV) Change Section	Contract Change Section	Pricing Table
Section Name	Internet Protocol Service Table of Contents	Access to Data and Information Service Ordering Trouble and Complaint Reporting Data Reporting Requirements Table of Contents	Proposal Notes	Pricing Overview Table of Contents	Section B	B.X.X.X B.X.X.X
File Name	v1_X-X-XX.doc v1-Contents.doc	v2_X-X,doc v2_X-X,doc v2_X-XX,doc v2_X-XX,doc v2-Contents.doc	V3-XX.doc	Narrative.doc V4-Contents.doc	Section B.doc	GSA Systems

The following is a summary of the changes contained in the submission:

- Volume I-Technical-Section X.X.XX.X entitled XXXXXXX was added on page 23 of the Internet Protocol Service of the contract.
- Volume II-Management-Section X.X.XX.X.X.X was added on pages 25-27 to identify responsibilities of the Service Operations Center, Trouble Reporting and Escalation Procedures. A statement regarding non-issuance of Trouble Status Reports was added to Table X.SS-S. XXXXXX has identified exceptions to the deliverable reporting data in Section X.SS and has acknowledged that information concerning are not integrated with the existing EISXXXXX systems.
- Volume III-Business-Section3, XXXXXX Service Terms and Conditions, has been updated to include the specific provisions for XXXXXX services.
- Volume IV-P-Table X.XX.X was added to show the feature XXXX Mechanisms and Feature Item Numbers for XXXX services.
- Price Table B.X.X-X and B.X.X-X were updated to include 27 CLINs for XXXX services.

APPENDIX C

Instructions for the Submission of Modifications

Overview

GSA Systems will use a relational database to maintain the up-to-date contract price information. Contractors will need to maintain a reliable relational database of the complete set of current prices that shall match with GSA Systems in terms of price and location tables, their formats and contents. The contractor shall maintain its connection to GSA Systems for the duration of the contract. The GSA Systems' database will be maintained by the government as its definitive repository of prices for the life of the EIS contract. The complete set of current prices shall include all prices in the contract including price changes due to contract modifications, plus prices resulting from approved TO-specific submissions and catalog submissions. The complete set of current contract prices will be used as the baseline for the preparation of proposed contract modifications that include potential future price changes to be included in the contract.

Proposed contract, TO-specific, and catalog prices:

- Shall exclude the GSA AGF
- Shall include all appropriate discounts
- Shall include the correct numerical precision (the correct number of digits after the decimal point)
- Shall not exceed those already on contract for the identical service

The term **submission** refers to a contractor-generated proposal for:

1. a contract modification,
2. a TO-specific submission, or
3. a catalog submission,

A successful contract modification submission will become a contract modification after the contracting officer's approval. At time of submission, the contractor will assign each submission a submission number in accordance with the "Submission Numbering Scheme" defined in Appendix A. Submissions that include more than one service may be delayed. The contractor shall submit contract modification submissions, TO-specific submissions, and catalog submissions, separately.

The contractor shall submit contract modification submissions, TO-specific submissions, and catalog submissions, (initial, interim and final) via GSA Systems.

Procedures

Submissions shall be incremental. That is, the submitted price change file will contain only tables that have been added or changed, and only rows within those tables that have been added, removed, or changed. Furthermore, any one submission shall contain only the changes for that one submission, not any combination of the current and previous submissions.

The contractor shall use a version number of "01" for the initial version of a submission. Subsequent versions of the submission shall not be incremental with respect to the previous version, but rather shall completely replace the previous version. The contractor shall ensure that any version submitted subsequent to the initial version is structured so that it contains a full and complete representation of the current state of the submission.

All price changes, price additions, and price deletions require the contractor to submit at least one row to each affected B-table. The submitted row(s) shall contain at a minimum the TO number[3], the CLIN, the price, the price start date and the price stop date.

All price tables include a price-replaced date column. This column is to be completed only by the government; the contractor shall not make an entry in the price replaced date column in its submissions. This column will remain NULL in all tables in the current contract schema (e.g. v0_eis). After award of any contract modification or approval of any TO-specific submission or catalog submission that changes a price table, the government will, as part of its process for integrating the awarded or approved price data, enter the date of execution into the price-replaced date column in all new rows created in the contract archive schema (e.g. v0_eis_archive).

Adding a New CLIN to an Existing Table[4]

To add a new CLIN to an existing table, the contractor must propose a contract modification to:

[3] For contract modification submissions, the contractor shall populate the TO Number column with "-1"

[4] New CLINs shall only be added via contract modification submissions, not via TO-specific submissions or catalog submissions

1. Define the new CLIN,
2. Identify which B-table the CLIN is in (and, if applicable, the location or combination of location values), and
3. Provide prices and effective dates for the new CLIN

To define the new CLIN, the contractor shall add a row in the “clin” table to define each new CLIN being added to the contract. The following are guidelines for defining a new CLIN:

- New CLIN descriptions should NOT contain the following:
  - Service ID or Service Name (e.g., PLS, Wireless, Voice Service)
  - Frequency (e.g., MRC, NRC, Usage)
- New CLIN descriptions should be structured and formatted like similar existing CLINs to aid users in distinguishing between similar, related CLINs. CLIN assignments should be chosen so that the CLINs of similar, related services fall within close proximity to one another in lists that are sorted by CLIN.

To define which B-table the CLIN is in (and, if applicable, the location or combination of location values) the contractor shall add a row in the “loc_base_input” table for each Btable_id for which the new CLIN is being added. For each new Btable_id, additional rows shall be added to indicate all valid location values or combinations of location values.

To provide the price(s) and effective dates for the new CLIN, the contractor shall submit at least one row for each affected B-table; the submitted row(s) shall contain a TO number of -1, the CLIN, the price for the CLIN, the price start date and the price stop date, along with any other parameters such as location values that are required for the B-table to fully differentiate the price.

Example

Table 1 represents the submission of the row to be added to the “clin” table to define a new CLIN. It includes the new CLIN, the description (name) of the new CLIN and several required characteristics of the CLIN.

clin	name	frequency	icb	nsp	unit_id	notes
MN11002	Managed Network Implementation, Maintenance and Management, Small	NRC	0	0	261	

Table 1: Submitted clin table

Table 2 shows the entry required in the “loc_base_input” table to identify the B-table(s) into which the new CLIN is to be inserted. This table defines CLIN MN11002 to be priced in Table B.2.8.1.3.1; the -1 entries in the loc1 and loc2 columns define that the CLIN is not location specific.

clin	btable_id	loc1	loc2
MN11002	28131	-1	-1

Table 2: Submitted loc_base_input table

Also, the TO number, CLIN, price(s), price start dates and price stop dates for the new CLIN must be added to the appropriate B-table(s). Table 3a below represents the state of the table prior to submission of the contract modification.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-09-30	
-1	MN11001	80	2019-10-01	2020-09-30	
-1	MN11001	60	2020-10-01	2027-09-30	

Table 3a: Contract B-table prior to Mod Submission

To add new CLIN MN11002 to the above table, with prices through the end of the contract, the contractor would submit the following table (Table 3b).

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11002	200	2017-10-01	2022-09-30	

Table 3b: Submitted B-table

This provides a price for the new CLIN from the price start date to the end of the first option period. Note that since this is a contract modification, not a TO-specific submission, the task order number column of the price table is populated with "-1".

After the contract modification is executed, the government will integrate the proposed modification. After integration of the modification, the revised Table B.2.8.1.3.1 would appear as shown below in Table 3c.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-09-30	
-1	MN11001	80	2019-10-01	2020-09-30	
-1	MN11001	60	2020-10-01	2022-09-30	
-1	MN11002	200	2017-10-01	2022-09-30	

Table 3c: Contract B-table After Mod Integration

Adding a New Price for an Existing CLIN to an Existing Table

To price an existing CLIN in an existing B-table, the contractor shall submit at least one pricing row for each affected B-table; the submitted row(s) shall contain the TO number[333], the CLIN, the price for the CLIN, the price start date and the price stop date, along with any other parameters such as location, that are required for that B-table to fully differentiate the price. If the CLIN has never been priced in the desired B-table, the contractor shall also include a "loc_base_input" table row in the submission for the B-table in which the CLIN is being priced for the first time.

Formatted: Footnote Reference

Formatted: Footnote Reference

Changing an Existing Price in a Table

To indicate a price change, the contractor shall submit new price rows to replace the existing prices. Note that all current and future dates covered by the replaced price row(s) shall be covered by the added row(s). That is, contractors shall take care not to create date “holes” in price coverage. Note that the new price shall be effective on the price start date.

Example

Table 4a below represents the state of the table prior to submission of the contract modification.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-09-30	
-1	MN11001	80	2019-10-01	2020-09-30	
-1	MN11001	60	2020-10-01	2022-09-30	
-1	MN11002	200	2017-10-01	2022-09-30	

Table 4a: Contract B-table prior to Mod Submissions

To reduce the price of CLIN MN11001 from the existing price of $100 to $90 for the period 2019-4-01 through 2019-09-30, the contractor would submit the following table with only one row as shown below (Table 4b).

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	90	2019-04-01	2019-09-30	

Table 4b: Submitted B-table

After award of the modification (e.g. the mod is executed on 2019-03-22), the government makes the necessary database adjustments to integrate the modification. After integration of the modification, the revised Table B.2.8.1.3.1 would appear as shown below (Table 4c). Notice that the government modified one row to change the

price stop date from 2019-09-30 to 2019-03-31 and then added a new row reflecting the price reduction, with a price start date of 2019-04-01.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-03-31	
-1	MN11001	90	2019-04-01	2019-09-30	
-1	MN11001	80	2019-10-01	2020-09-30	
-1	MN11001	60	2020-10-01	2022-09-30	
-1	MN11002	200	2017-10-01	2022-09-30	

Table 4c: Contract B-table After Mod Integration

In addition, the following would be added by the government to Table B.2.8.1.3.1 in the contract archive schema.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices (archive)

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-09-30	2019-03-22

Table 4d: Row Added to Archive B-table After Mod Integration

Adding a Task Order-Specific Price

The procedure for adding a TO-specific price is similar to that of adding a new price for an existing CLIN to an existing table. The difference is that the contractor shall populate the task order number column with a valid TO number rather than “-1”. For example, starting with Table 4c from above, the contractor could include the following Table 5a in a TO-specific submission.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
SS00-34-90186	MN11002	190	2019-05-01	2022-09-30	

Table 5a: Submitted B-table

After integration of the submission, the revised Table B.2.8.1.3.1 would appear as shown below (Table 5b).

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-03-31	
-1	MN11001	90	2019-04-01	2019-09-30	
-1	MN11001	80	2019-10-01	2020-09-30	
-1	MN11001	60	2020-10-01	2022-09-30	
-1	MN11002	200	2017-10-01	2022-09-30	
SS00-34-90186	MN11002	190	2019-05-01	2022-09-30	

Table 5b Contract: B-table After Task Order-Specific Submission Integration

Deleting a Price

To submit a price for deletion, the contractor shall include the row in the submission with the price start date and the price stop date both set to the last day of the month the CLIN will be available. Note that the last date the price shall be in effect is on the price stop date.

Example

Using Table 4c above as a starting point, if the contractor proposes to delete pricing for CLIN MN11001 effective at the end of calendar year 2021, the contractor would submit the following table with only one row as shown below (Table 6a).

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	60	2021-12-31	2021-12-31	

Table 6a: Submitted B-table

After award of the modification, the government makes the necessary database adjustments to integrate the modification. After integration of the modification, the new Table B.2.8.1.3.1 would appear as shown below (Table 6b). Notice that the government modified one row to change the price stop date from 2022-09-30 to 2021-12-31.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	100	2017-10-01	2019-03-31	
-1	MN11001	90	2019-04-01	2019-09-30	
-1	MN11001	80	2019-10-01	2020-09-30	
-1	MN11001	60	2020-10-01	2021-12-31	
-1	MN11002	200	2017-10-01	2022-09-30	

Table 6b: Contract B-table After Mod Integration

In addition, the following would be added by the government to Table B.2.8.1.3.1 in the contract archive schema.

Table B.2.8.1.3.1: Managed Network Implementation, Management and Maintenance Prices (archive)

task order number	clin	price	price start date	price stop date	price replaced date
-1	MN11001	60	2020-10-01	2022-09-30	(Mod Award Date)

Table 6c: Row Added to Archive B-table After Mod Integration

Adding a Catalog Item

The procedure for adding a catalog item is similar to that of adding a new price for an existing CLIN to an existing table. The difference is that the contractor shall populate the appropriate catalog tables. Below is an example of adding a catalog item for SRE associated with Device Class ID 6123. Other catalog items listed in Section B.1.3 should be added in similar fashion.

Table B.2.10.2.1: SRE Catalog – Product Specification Table

CLIN	Case Number	SRE Type	Manufacturer	Model No.	Part No.	UPC	Model/Part Description	Device Size	Rated for Energy Efficiency Compliance	Energy Efficiency Standards and Ratings	OLP	No List Price	Device Class ID	SRE MRC Options	Start Date	Stop Date	End of Sale Date	End of Life Date	Notes
EQ9000 1	0001	S	CISCO	N/A	CISCO1941W-A/K9		Cisco 1941 Router w/ 802.11 a/b/g/n FCC Compliant WLAN ISM	2	Y	EPEAT	$2095.00		6123	{24,36}	2019-10-01	2020-09-30			

Table 7a: Submitted B-table

Date Constraints

Price start and stop dates are not constrained to contract year boundaries. However, prices must start on the first day of a month and stop on the last day of a month. The price start date shall not be earlier than the date of the modification submission.

Adding a New Price Table

The format of a new price table must be reviewed and approved by the government prior to the submission of a modification. It should follow the basic guidelines of all current price tables, such as including columns for the TO number, CLIN, price, and start, stop and replace dates.

Submission Contents

All submissions must be submitted as specified below:

1) Tables in pre-approved price table formats
2) Tables stored in GSA Systems

At both the contractor's and the government's discretion, government resources may be made available to assist the contractor in the preparation of a submission (particularly, when a new price table format is involved). All proposals for contract modification

submissions, TO-specific submissions, and catalog submissions, that contain pricing data shall comply with these submission requirements; those that do not will be returned to the contractor unprocessed.

Verification Mechanism

The government will publish general reference information useful for preparing the price submission such as country/jurisdiction IDs, services, service types and categories, price table formats, valid start and stop dates, charging units, etc. The contractor shall reference this information before preparing its new submission to GSA. If the contractor needs any information that does not exist in the published material, such as country codes, charging units, or table formats, then GSA will provide that information.

The government may also provide pre-submission support to the contractor to verify its submission for correctness. This support consists of validating price tables (their names, table_ids, formats), price dates, and verifying new CLINs for uniqueness and details.

J.5 Labor Categories

All labor categories are based on the Office of Management and Budget's (OMB) Standard Occupational Classification (SOC), as supplemented by the Bureau of Labor Statistics (BLS) Department of Labor Employment and Training Administration's Occupational Information Network (O*NET) (http://online.onetcenter.org). More detailed information on each labor category, including required skills, knowledge, and tool experience, can be found on the O*NET website.

The SOC code is indicated for each labor category. Refer to section B.2.11.2, Labor Categories, for more information on the use of SOC codes in this contract. Also indicated for each labor category is the Occupational Group from the BLS Employment Cost Index to be used in determining price escalation factors. Refer to Section H.19 for information on labor price escalation.

The following labor categories are included in this contract.

Business Continuity Planner (SOC Code 13-1199.04; Occupational Group "Professional and related")

Develop, maintain, or implement business continuity and disaster recovery strategies and solutions, including risk assessments, business impact analyses, strategy selection, and documentation of business continuity and disaster recovery procedures. Plan, conduct, and debrief regular mock-disaster exercises to test the adequacy of existing plans and strategies, updating procedures and plans regularly. Act as a coordinator for continuity efforts after a disruption event.

Computer Network Architect (SOC Code 15-1143.00; Occupational Group "Professional and related")

Design and implement computer and information networks, such as local area networks (LAN), wide area networks (WAN), intranets, extranets, and other data communications networks. Perform network modeling, analysis, and planning. May also design network and computer security measures. May research and recommend network and data communications hardware and software.

Computer Network Support Specialist (SOC Code 15-1152.00; Occupational Group "Professional and related")

Analyze, test, troubleshoot, and evaluate existing network systems, such as local area network (LAN), wide area network (WAN), and Internet systems or a segment of a network system. Perform network maintenance to ensure networks operate correctly with minimal interruption.

Computer Systems Analyst (SOC Code 15-1121.00; Occupational Group "Professional and related")

Analyze science, engineering, business, and other data processing problems to implement and improve computer systems. Analyze user requirements, procedures, and problems to automate or improve existing systems and review computer system capabilities, workflow, and scheduling limitations. May analyze or recommend commercially available software.

Computer Systems Engineers/Architect (SOC Code 15-1199.02; Occupational Group "Professional and related")

Design and develop solutions to complex applications problems, system administration issues, or network concerns. Perform systems management and integration functions.

Customer Service Representatives (SOC Code 43-4051.00; Occupational Group "Service Occupations")

Interact with customers to provide information in response to inquiries about products and services and to handle and resolve complaints.

Database Administrator (SOC Code 15-1141.00; Occupational Group "Professional and related")

Administer, test, and implement computer databases, applying knowledge of database management systems. Coordinate changes to computer databases. May plan, coordinate, and implement security measures to safeguard computer databases.

Database Architect (SOC Code 15-1199.06; Occupational Group "Professional and related")

Design strategies for enterprise database systems and set standards for operations, programming, and security. Design and construct large relational databases. Integrate new systems with existing warehouse structure and refine system performance and functionality.

Electrical Drafter – Computer Aided Design (CAD) Operator (SOC Code 17-302.02; Occupational Group "Professional and related")

Prepare wiring diagrams, circuit board assembly diagrams, and layout drawings used for the manufacture, installation, or repair of electrical equipment.

Information Security Analyst (SOC Code 15-1122.00; Occupational Group "Professional and related")

Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses.

Information Technology Project Manager (SOC Code 15-1199.09; Occupational Group "Management, business, and financial")

Plan, initiate, and manage information technology (IT) projects. Lead and guide the work of technical staff. Serve as liaison between business and technical aspects of projects. Plan project stages and assess business implications for each stage. Monitor progress to assure deadlines, standards, and cost targets are met.

Network and Computer Systems Administrator (SOC Code 15-1142.00; Occupational Group "Professional and related")

Install, configure, and support an organization's local area network (LAN), wide area network (WAN), and Internet systems or a segment of a network system. Monitor network to ensure network availability to all system users and may perform necessary maintenance to support network availability. May monitor and test Web site performance to ensure Web sites operate correctly and without interruption. May assist in network modeling, analysis, planning, and coordination between network and data communications hardware and software. May supervise computer user support specialists and computer network support specialists. May administer network security measures.

Software Developer – Applications (SOC Code 15-1132.00; Occupational Group "Professional and related")

Develop, create, and modify general computer applications software or specialized utility programs. Analyze user needs and develop software solutions. Design software or customize software for client use with the aim of optimizing operational efficiency. May analyze and design databases within an application area, working individually or coordinating database development as part of a team. May supervise computer programmers.

Software Developer – Systems Software (SOC Code 15-1133.00; Occupational Group "Professional and related")

Research, design, develop, and test operating systems-level software, compilers, and network distribution software for medical, industrial, military, communications, aerospace, business, scientific, and general computing applications. Set operational specifications and formulate and analyze software requirements. May design embedded systems software. Apply principles and techniques of computer science, engineering, and mathematical analysis.

Software Quality Assurance Engineer/Tester (SOC Code 15-1199.01; Occupational Group "Professional and related")

Develop and execute software test plans in order to identify software problems and their causes.

Sustainability Specialist (SOC Code 13-1199.05; Occupational Group "Professional and related")

Address organizational sustainability issues, such as waste stream management, green building practices, and green procurement plans.

Telecommunications Engineering Specialist (SOC Code 15-1143.01; Occupational Group "Professional and related")

Design or configure voice, video, and data communications systems. Supervise installation and post-installation service and maintenance.

Telecommunications Equipment Installer/Repairer (SOC Code 49-2022.00; Occupational Group "Service Occupations")

Install, set-up, rearrange, or remove switching, distribution, routing, and dialing equipment used in central offices or headends. Service or repair telephone, cable television, Internet, and other communications equipment on customers' property. May install communications equipment or communications wiring in buildings.

Telecommunications Line Installer/Repairer (SOC Code 49-9052.00); Occupational Group "Service Occupations")

Install and repair telecommunications cable, including fiber optics.

Web Administrators (SOC Code 15-1199.03; Occupational Group "Professional and related")

Manage web environment design, deployment, development and maintenance activities. Perform testing and quality assurance of websites and web applications.

Web Developers (SOC Code 15-1134.00; Occupational Group "Professional and related")

Design, create, and modify Web sites. Analyze user needs to implement Web site content, graphics, performance, and capacity. May integrate Web sites with other computer applications. May convert written, graphic, audio, and video components to compatible Web formats by using software designed to facilitate the creation of Web and multimedia content.

J.6 GSA CIO IT Security Guides

J.7 GSA IT Security Directives and Instructional Letters

J.8 Security Assessment Document Templates

J.9 Site Survey Estimate Template for Wiring Install

Site Survey Estimate Template for Wiring Install*							**Version 1.0**
Quote Date:							
Quote Expiration Date:							
Service Location:							
Location ID: (include NSC)							
Contractor:							
Solicitation and/or Task Order No.:							
Install Description (Demarc Extension, New install, etc.)							
Attach Drawing, if applicable							
Attach Quote, if applicable							
Construction and Equipment Costs*							
Service/Product	**Description**	**Manufacturer/Part Number, Labor Category, where applicable**	**Qty**	**Unit (feet, hours, etc.)**	**Unit Price**	**Total**	**Price Source, if applicable**
Cable/Fiber (list type, strands, length)							
Conduit/Duct (list type and length)							
Installation - (Per Foot)							
Plowing							
Directional Boring - (Rural, Urban, Rock)							
Hand holes							
Hand hole Installation							

Firewall Penetration							
Equipment/Material							
Add Itemized Materials as needed							
Labor and Other Costs*							
Service/Product	**Description**	**Manufacturer/Part Number, Labor Category, where applicable**	**Qty**	**Unit (feet, hours, etc.)**	**Unit Price**	**Total**	**Price Source, if applicable**
List Labor Categories**, hours, and work to be performed							
Permits							
Other Incidental Elements that may contribute to price (provide detail)							
Total Estimated Project Cost							

* Categories may be left blank, modified, or added to provide a detailed estimate sufficient to support a fair and reasonable determination
** To the extent possible, include labor categories and rates from Section B.2.11

J.10 Site Survey Estimate Template for Special Access Construction

Site Survey Estimate Template for Special Access Construction*							**Version 1.0**
Quote Date:							
Quote Expiration Date:							
Service Location:							
Location ID: (include NSC)							
Contractor:							
Solicitation and/or Task Order No.:							
Type of Service (DS3, OC3, Ethernet, etc.)							
Attach Drawing							
Attach Contractor Quote							
Construction and Equipment Costs*							
Service/Product	**Description**	**Manufacturer/Part Number, Labor Category, where applicable**	**Qty**	**Unit (feet, hours, etc.)**	**Unit Price**	**Total**	**Price Source, if applicable**
Cable/Fiber (list type, strands, length)							
Conduit/Duct (list type and length)							
Installation - (Per Foot)							
Plowing							
Directional Boring - (Rural, Urban, Rock)							
Hand holes							
Hand hole Installation							

Equipment (FW4100 ES, Fiber Distribution Panel, NIUs, etc.)							
Equipment Rentals							
Additional Equipment (provide detail)							
Labor and Other Costs*							
Service/Product	**Description**	**Manufacturer/Part Number, Labor Category, where applicable**	**Qty**	**Unit (feet, hours, etc.)**	**Unit Price**	**Total**	**Price Source, if applicable**
List Labor Categories**, hours, and work to be performed							
Design							
Permits							
Traffic Control							
Mobilization							
Engineering							
Administration							
Other Incidental Elements that may contribute to price (provide detail)							
Total Estimated Project Cost							

* Categories may be left blank, modified, or added to provide a detailed estimate sufficient to support a fair and reasonable determination
** To the extent possible, include labor categories and rates from Section B.2.11

J.11 Abbreviations and Acronyms

J.11.1 Abbreviations and Acronyms Table

Abbreviation or Acronym	Definition
A	
A&A	Assessment and Authorization
AA	Access Arrangement
ACO	Administrative Contracting Officer
ACS	Audio Conferencing Service
ACT	Accounting Control Transaction
AD	Agency Dispute
ADSL	Asymmetric DSL
AGF	Associated Government Fee
AGFD	AGF Detail
AHC	Agency Hierarchy Code
AHS	Application Hosting Services
AIS	Automated Information System
ANI	Automatic Number Identification
ANSI	American National Standards Institute
Anti-DDoS	Anti-Distributed Denial of Service
AO	Authorizing Official
AOW	Area of the World
API	Application Programming Interface
APS	Automatic Protection Switching
ARIN	American Registry for Internet Numbers
AQL	Acceptable Quality Level
AS	Autonomous System
ASC	Accredited Standards Committee
ASCII	American Standard Code for Information Interchange
ASCO	Adversarial Supply Chain Operation
ASON	Automatic Switched Optical Network
ASP	Applications Services Provider
ASRN	Agency Service Request Number

Abbreviation or Acronym	Definition
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
ATO	Authority to Operate
ATR	AGF Electronic Funds Transfer Report
AU	Authorized Users
AUP	Acceptable Use Policy
Av(S)	Availability (Service)
AVI	Audio Visual Interleave
AVM	Anti-Virus Management
AVMS	Anti-Virus Management Service
B	
B2B	Business to Business
BA	Billing Adjustment
BI	Billing Invoice
BER	Bit Error Rate
BGAN	Broadband Global Area Network
BGP	Boarder Gateway Protocol
BIA	Business Impact Assessment
BIT	Binary Digit
BLS	Bureau of Labor Statistics
BoD	Bandwidth on Demand
BLSR	Bidirectional Line Switched Ring
BPS	Bits per second
BPSR	Bidirectional Path Switched Ring
BRI	Basic Rate Interface
BSD	Boundary Scope Document
BSS	Broadband Switching System
BSS	Business Support System
BTN	Billing Telephone Number
BYOD	Bring Your Own Device
C	
CA	Criticality analysis

Abbreviation or Acronym	Definition
CAC	Common Access Card
CAGE	Commercial and Government Entity
CAP	Compliance and Assurance Program
CBR	Constant Bit Rate
CBS	Committed Burst Size
CBSA	Core Based Statistical Area
CCCS	Customer Contact Center Services
CCE	Common Configuration Enumerations
CCS	Contact Center Service
CCV	Cybersecurity Compliance Validation
CDIP	Contractor Data Interaction Plan
CDMA	Code Division Multiple Access
CDN	Content Delivery Network
CDNS	Content Delivery Network Service
CDP	Carbon Disclosure Project
CDR	Call Detail Record
CDRL	Contract Deliverables Requirements List
CE	Customer Edge
CFR	Code of Federal Regulations
CFSS	Commercial Fixed Satellite Service
CGI-Bin	Common Graphic Interface - Binary
CID	Caller ID
CIR	Committed Information Rate
CIRs	Committed Information Rates
CIS	Center for Internet Security
CLIN	Contract Line Item Number
CLLI	Common Language Location Identifier
CLONES	Central Location Online Entry System (iconectiv database)
CMSS	Commercial Mobile Satellite Service
CNAM	Calling Name
CNM	Customer Network Management
CNSS	Committee on National Security Systems

Abbreviation or Acronym	Definition
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CO	Contracting Officer
COMSATCOM	Commercial Satellite Communication
CONUS	Continental United States
COOP	Continuity of Operations
COR	Contracting Officer's Representative
CoS	Class of Service
CoSS	Collaboration Support Services
COTS	Commercial off-the-shelf
CP	Contingency Plan
CPDF	Central Personnel Data File
CPE	Customer Premises Equipment
CPLG	Coupling
CPMO	Contractor's Program Management Office
CPTP	Contingency Plan Test Plan
CPTPR	Contingency Plan Test Plan Report
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSA	Communications Service Authorization
CSC	Customer Service Center
CSDS	Circuit Switched Data Service
CSO	Customer Support Office
CSP	Communications Service Provider
CSRN	Contractor Service Request Number
CSS	Circuit Switched Service
CSTA	Computer Supported Telephony Applications
CSU/DSU	Channel Service Unit/Data Service Unit
CSV	Comma-Separated Value
CSVS	Circuit Switched Voice Service
CTI	Computer Telephony Integration
CUI	Controlled Unclassified Information

Abbreviation or Acronym	Definition
CVE	Common Vulnerabilities and Exposures
CW	Cable and Wiring
CWD	Customer Want Date
D	
D/A	Departments and Agencies
DBA	Doing Business As
DBAS	Direct Billed Agency Setup
DCC	Data Communications Channel
DCOM	Distributed Component Object Model
DCS	Data Center Service
DCSS	Digital Cross-Connect Systems
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DFS	Dark Fiber Service
DHCP	Dynamic Host Configuration Protocol
DHS	Dedicated Hosting Service
DID	Direct Inward Dial
DIS	Draft International Standard
DLCI	Data Link Connection Identifier
DLP	Data Loss Prevention
DLS	Data Link Switching
DM	Degraded Minutes
DMS	Defense Message System
DMZ	Demilitarized Zones
DNBH	During Normal Business Hours
DNI	Dialed Number Identification
DNIS	Dialed Number Identification Service
DNS	Domain Name System
DNSSEC	DNS Security Extensions
DoD	Department of Defense
DoDI	Department of Defense Instruction
DoS	Denial of Service

Abbreviation or Acronym	Definition
DPA	Delegation of Procurement Authority
DR	Disaster Recovery
DR	Dispute Report
DSL	Digital Subscriber Line
DSN	Defense Switched Network
DSSR	Department of State Standardized Regulations
DSU	Data Service Unit
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-Frequency
DUNS	Data Universal Numbering System
DWDM	Dense Wavelength Division Multiplexing
E	
EAD	Enterprise Active Directory
ECS	Electronic Commerce Service
EFMA	Ethernet in the First Mile Alliance
EFS	Error Free Seconds
EFT	Electronic Funds Transfer
E-Gov	Electronic Government
EIA	Electronic Industries Association
EIA/TIA	Electronic Industry Alliance/Telecommunications Industry Association
EIS	Enterprise Infrastructure Solutions
EIT	Electronic and Information Technology
E-LAN	Ethernet Private Local Area Network
E-LINE	Ethernet Private Line
EM	Element Manager
EMI	Electro-Magnetic Interference
EMS	Element Management Systems
EN	Event Notification
EO	Executive Order
EP	Emergency Preparedness
EPA	Environmental Protection Agency
ERM	E-mail Response Management

Abbreviation or Acronym	Definition
ERP	Enterprise Resource Planning
ESCON	Enterprise System Connection
ESF	Extended Superframe
ESI	Electronically Stored Information
ETL	Extract, Transform and Load
ETS	Ethernet Transport Service
ETSI	European Telecommunications Standards Institute
EVC	Ethernet Virtual Connection
F	
FAR	Federal Acquisition Regulation
FB	Fixed Bandwidth
FCC	Federal Communications Commission
FCCI	Federal Cloud Computing Initiative
FCIA	Fiber Channel Industry Association
FDCCI	Federal Data Center Consolidation Initiative
FDP	Fiber Distribution Panel
FEDBIZOPPS	Federal Business Opportunities
FedRAMP	Federal Risk and Authorization Management Program
FED-STD	Federal Standard
FedVRS	Federal Video Relay Service
FEMP	Federal Energy Management Program
FICON	Fiber Connectivity
FIPS	Federal Information Processing Standard
FIPS 200	Federal Information Processing Standards Publication 200
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
FLSA	Fair Labor Standards Act
FOC	Firm Order Commitment
FOCN	Firm Order Commitment Notice
FOIA	Freedom of Information Act
FS	Federation Services
FSDP	Fiber Service Delivery Point

Abbreviation or Acronym	Definition
FT1	Fractional T1
FT3	Fractional T3
FTP	File Transfer Protocol
FTR	Federal Telecommunications Recommendations
FTTP	Fiber to the Premises
FUSF	Federal Universal Service Fund
G	
GAO	General Accounting Office
GB	Gigabyte
Gbps	Gigabit per second
GETS	Government Emergency Telecommunications Service
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFP	Government Furnished Property
GFP	Generic Framing Procedure
GMPLS	Generalized Multi-Protocol Label Switching
GOS	Grade of Service
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GRI	Global Reporting Initiative
GSA	General Services Administration
GSAR	GSA Regulation
GUI	Graphical User Interface
H	
HCM	Human Capital Management
HF	High Frequency
HIDS	Host-based IDS
HR	Human Resources
HSPD-12	Homeland Security Presidential Directive-12
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol

Abbreviation or Acronym	Definition
HVAC	Heating, Ventilation and Air Conditioning
I	
IA	Interagency Agreement
IaaS	Infrastructure as a Service
ICB	Individual Case Basis
ICE	Interactive Connectivity Establishment
ICMP	Internet Control Message Protocol
ID	Identification (User)
IDC	Internet Data Center
IDE	Integrated Development Environment
IDPS	Intrusion Detection and Prevention Service
IDS	Intrusion Detection System
IDSL	ISDN DSL
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IETF RFC	IETF Request for Comment
IMAP	Internet Message Access Protocol
INRS	Incident Response Service
IP	Internet Protocol
IPFIX	IP Flow Information Export
IPMS	Integrated Performance Monitoring Service
IPS	Internet Protocol Service
IPSec	IP Security
IPS	Intrusion Prevention Systems
IPSS	Intrusion Prevention Security Service
IPVS	Internet Protocol Voice Service
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IR1-SLM	Intermediate Reach Single Longitudinal Mode
IR	Inventory Reconciliation
IRP	Incident Response Plan

Abbreviation or Acronym	Definition
IRS	Internal Revenue Service
IRU	Indefeasible Rights of Use
ISA	Interconnection Security Agreements
ISCM	Information Security Continuous Monitoring
ISDN	Integrated Services Digital Network
ISDN BRI	ISDN Basic Rate Interface
ISM	In-Service Monitoring
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSM	Information Systems Security Manager
ISSO	Information System Security Officer
ISV	Independent Software Vendor
ITIL	IT Infrastructure Library
ITS	Integrated Technology Services
ITSM	IT Service Management
ITT	Information Technology Tools
ITU	International Telecommunications Union
ITU-TSS	International Telecommunications Union-Telecommunications Service Sector
IVR	Interactive Voice Response
K	
KPI	Key Performance Indicator
L	
L2TP	Layer 2 Tunneling Protocol
L3VPN	Layer 3 Virtual Private Network
LAN	Local Area Network
Latency(S)	Latency (Service)
LCAS	Link Capacity Adjustment Scheme
LDAP	Lightweight Directory Access Protocol
LEC	Local Exchange Carrier
LGC	Local Government Contact
LH	Long Haul
LLDS	Link Layer Data Service

Abbreviation or Acronym	Definition
LNP	Local Number Portability
LOA	Letter of Authorization
LOH	Line Overhead
LR1-SLM	Long Reach Single Longitudinal Mode
LSA	Local Service Agreement
LSP	Label Switched Paths
LTE	Long Term Evolution
M	
M2M	Machine to Machine
MACD	Moves, Adds, Changes, Disconnects
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MAS	Mobile Application Store
MB	Megabyte
MBI	Minimum Background Investigation
Mbps	Megabit per second
MBS	Maximum Burst Size
MCM	Mobil Content Management
MDM	Mobile Device management
MEF	Metro Ethernet Forum
MFS	Managed Firewall Service
MIL-STD	Military Standard
MIME	Multipurpose Internet Mail Extensions
MLPP	Multi-Level Precedence and Preemption
MMC	Monthly Maintenance Charge
MMF	Multi-Mode optical Fiber
MMRC	Maintenance Monthly Recurring Cost
MMS	Multimedia Messaging Service
MNS	Managed Network Service
MOS	Mean Opinion Score
MPIN	Marketing Partner Identification Number
MPLS	Multi-Protocol Label Switching

Abbreviation or Acronym	Definition
MPS	Managed Prevention Service
MRC	Monthly Recurring Charges
MRG	Minimum Revenue Guarantee
MS	Microsoft
MSS	Managed Security Service
MTIPS	Managed Trusted Internet Protocol Service
MTTLBCI	Mean Time to Loss of BCI
MUX	Multiplexer
MWS	Wireless Service
N	
NACI	National Agency Check with Written Inquiries
NACSZ	Name, Address, City, State, Zip code
NAICS	North American Industry Classification System
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NCPS	National Cyber Protection System Sensor
NCS	National Communications System
NDA	Non-Disclosure Agreement
NEBS	Network Equipment-Building System
NFC	Near Field Communication
NFS	Network File Systems
NFV/SDN	Network Function Virtualization and Software Defined Network
NIC	Network Interface Card
NIDS	Network Intrusion Detection Devices
NIS	Network Information Service
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NLT	Not Later Than
NMS	Network Management System
NNI	Network to Network Interface
NOC	Network Operations Center

Abbreviation or Acronym	Definition
NPA	Numbering Plan Area
NPA/NXX	Numbering Plan Area / Numbering Plan Exchange
NRC	Non-Recurring Charge
NS	National Security
NS/EP	National Security and Emergency Preparedness
NS2020	Network Services 2020
NSA	National Security Agency
NSC	Network Site Code
NSP	Not Separately Priced
NTSC	National Television Standards Committee
NUI	Network User Identification
NVF	Network Function Virtualization
NXX	Numbering Plan Exchange
NZDS	Non-Zero Dispersion Shifted
O	
O&S	Operations and Support
O*NET	Occupational Information Network
OADM	Optical Add-Drop Multiplexer
OAM	Operations, Administration and Management
OAM&P	Operations, Administration, Maintenance and Provisioning
OCN	Operating Company Number
OCO	Ordering Contracting Officer
OCONUS	Outside Contiguous United States
OCWR	Optical Continuous Wave Reflectometry
OEC	Office of Emergency Communication
OEM	Original Equipment Manufacture
OFCS	Optical Fiber Communications System
OFSTP	Optical Fiber System Test Procedure
OIF	Optical Internetworking Forum
OLP	Official List Price
OMB	Office of Management and Budget
ONBH	Outside Normal Business Hours

Abbreviation or Acronym	Definition
OOS	Out-Of-Service
OPM	Office of Personnel Management
OS	Operating System
OSAISO	Office of the Senior Agency Information Security Officer
OTDR	Optical Time-Domain Reflectometer
OTM	Optical Terminal Multiplexer
OTN	Optical Transport Network
OVF	Open Virtualization Format
OVPN	Optical Virtual Private Network
OWS	Optical Wavelength Service
P	
P&P	Policies and Procedures
PaaS	Platform as a Service
PAL	Phase Alternation by Line
PAT	Port Address Translation
PBX	Private Branch Exchange
PC	Personal Computer
PCL	Physical Concentration Location
PDF	Portable Document Format
PDU	Protocol Data Unit
PHub	Pricing Hub
PIA	Privacy Impact Assessment
PIC	Presubscribed Interexchange Carrier
PIDF	Presence Information Data Format
PII	Personally Identifiable Information
PIID	Procurement Instrument Identifier
PIM	Personal Information Management
PIN	Personal Identification Number
PIR	Peak Information Rate
PIV	Personal Identity Verification
PKI	Public Key Encryption
PLS	Private Line Service

Abbreviation or Acronym	Definition
PM	Performance Monitoring
PMD	Polarization Mode Dispersion
PMO	Program Management Office
PMP	Program Management Plan
POA&M	Plan of Action and Milestones
POC	Point of Contact
PoE	Power over Ethernet
PON	Passive Optical Networks
POP	Point of Presence
PPIRS	Past Performance Information Retrieval System
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
PRI	Primary Rate Interface
PS/ALI	Private Switch/Automatic Location Identification
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTT	Push to Talk
PVC	Permanent Virtual Circuit
PWE	Pseudo Wire Emulation
PWE3	Pseudo Wire Emulation Edge to Edge
PWS	Performance Work Statement
Q	
QA	Quality Assurance
QoS	Quality of Service
QPMR	Quarterly Program Management Review
R	
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
RFC	Request for Comment
RFI	Request for Information
RFI	Radio Frequency Interference
RFP	Request for Proposal

Abbreviation or Acronym	Definition
RFQ	Request for Quotation
RMF	Risk Management Framework
RoB	Rules of Behavior
RPC	Remote Procedure Call
RPR	Resilient Packet Rings
RT	Response Time
RTP	Real-Time Transport Protocol
RTT	Radio Transmission Technology
S	
SaaS	Software as a Service
SAM	System for Award Management
SAN	Storage Area Networks
SAR	Security/Risk Assessment Report
SC(O)	Switched Connection (Optical)
SCAP	Security Content Automation Protocol
SCCP	Skinny Client Control Protocol
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCOM	System Center Operations Manager
SCRM	Supply Chain Risk Management
SD	Signal Degradation
SDH	Synchronous Digital Hierarchy
SDK	Software Development Kit
SDN	Software Defined Network
SDP	Service Delivery Point
SDS	Switched Data Service
SDSL	Symmetric DSL
SECAM	Système Electronique Couleur Avec Memoire
SES	Severely Errored Seconds
SF	Super Frame
SF	Signal Failure
SFTP	Secure File Transport Protocol

Abbreviation or Acronym	Definition
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SIS	Satellite Internet Service
SLA	Service Level Agreement
SLACR	SLA Credit Request
SLACRR	SLA Credit Request Response
SLAR	SLA Report
SMB	Server Message Block
SME	Subject Matter Expert
SMF	Single Mode optical Fiber
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SO	Service Order
SOA	Service Order Acknowledgement
SOAC	Service Order Administrative Change
SOC	Security Operations Center; Service Order Confirmation
SOCN	Service Order Completion Notice
SORN	Service Order Rejection Notice
SOH	Section Overhead
SONET	Synchronous Optical Network
SONET ADM	SONET Add-Drop Multiplexer
SOO	Statement of Objective
SOW	Statement of Work
SP	Special Publication
SR	Short Reach
SRE	Service Related Equipment
SRG	Security Requirements Guide
SR-MLM	Short Reach Multi-Longitudinal Mode
SS	Storage Service
SSCN	Service State Change Notice
SSH	Secure Shell
SSL	Secure Sockets Layer

Abbreviation or Acronym	Definition
SSL/TLS	Secure Sockets Layer/Transport Layer Security
SSM	Synchronous Status Messaging
SSP	System Security Plan
STP	Shielded Twisted Pair
STUN	Session Traversal Utilities for NAT
SVC	Switched Virtual Circuit
SWC	Serving Wire Center
SWOT	Strengths, Weaknesses, Opportunities and Threats
T	
TACACS	Terminal Access Controller Access Control System
TAX	Tax Detail
TB	Terabyte
TBD	To Be Determined
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Telecommunications Device for the Deaf
TDD/TTY	Telecommunications Device for the Deaf/Teletypewriter
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TEMS	Telecommunications Expense Management Service
TESP	Telecommunications Electric Service Priority
TFS	Toll Free Service
TICAP	Trusted Internet Connection Access Provider
TIC	Trusted Internet Connection
TIN	Taxpayer Identification Number
TLS	Transport Layer Security
TMSAD	Trust Model for Security Automation Data
TO	Task Order
TOH	Transport Overhead
TOPP	Task Order Project Plan
TP	Transition Plan
TSGR	Transport Systems Generic Requirements
TSMP	Transition Strategy and Management Plan

Abbreviation or Acronym	Definition
TSP	Telecommunications Service Priority
TS/SCI	Top Secret/Sensitive Compartmented Informaiton
TTR	Time to Restore
TUC	Task Order Unique CLIN
U	
UBI	Unique Billing Identifier
UCS	Unified Communications Service
UI	User Interface
UIFN	Universal International Free Phone Number
UM	Unified Messaging
UMTS	Universal Mobile Telecommunications System
UNI	User-to-Network Interface
UPS	Uninterruptible Power System
UPSR	Unidirectional Path Switched Ring
URL	Universal Resource Locator
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team
USDA	United States Department of Agriculture
UTC	Coordinated Universal Time
UTP	Unshielded Twisted Pair
V	
V&H	Vertical and Horizontal
VBR	Variable Bit Rate
VESDA	Very Early Smoke Detection Apparatus
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VoIPTS	Voice over Internet Protocol Transport Service
VPAT	Voluntary Product Accessibility Template
VPN	Virtual Private Network
VPNS	Virtual Private Network Service
VS	Voice Service
VSAT	Very Small Aperture Terminal

Abbreviation or Acronym	Definition
VSR	Very Short Reach
VSS	Vulnerability Scanning Service
VT	Virtual Tributary
VTN	Virtual Telephone Number
VTS	Video Teleconferencing Service
VXML	Voice Extensible Markup Language
W	
WAN	Wide Area Network
WAP	Wireless Application Protocol
WCS	Web Conferencing Service
WDM	Wavelength Division Multiplexing
WEP	Wired Equivalent Privacy
WFM	Workforce Management
WLAN	Wireless Local Area Network
WMI	Windows Management Instrumentation
WPA	Wi-Fi Protected Access
WPS	Wireless Priority Service
WSDL	Web Service Definition Language
WWW	World Wide Web
X	
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
XSD	XML Schema Definition
XTACACS	Extended TACACS

J.12 Glossary of Terms

12x5 Support - Shall include the core hour coverage of 8AM – 7PM Eastern Time Monday – Friday
24x7 - Twenty-four hours a day, seven days a week, without exception (e.g., national holidays are not excluded).
3rd Generation Partnership Project (3GPP) - An agreement formed in December 1998 by several telecommunications standard bodies to create technical specifications for the International Telecommunication Union's third-generation standards; represented in the group are companies from China, Europe, Japan, Korea, and the United States.
Acceptable Quality Level (AQL) - The performance level guaranteed by the contractor for each KPI associated with an EIS service.
Access - The facility-based service arrangements that provide net locations and their associated points of connection with the transport service providers, known as Points of Presence (POPs).
Access Circuit - A dedicated facility, varying by type (e.g., analog, digital signal, or synchronous optical network) and by bandwidth, used to carry service(s) between an SDP and its POP.
Access Control - The process of limiting access to the resources of a system only to authorized personnel, programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.
Access Type - The type of access being provided. Five access types are defined for EIS: 1. Wireline Access, 2. Ethernet Access, 3. Cable Access, 4. Fiber to the Premises (FTTP), 5. Wireless Access.
Ad Hoc Reporting - The generation of reports at sporadic intervals with varying contents and purposes.
Advanced Encryption Standard (AES) - Symmetric key cryptographic standard published by NIST. Uses 128, 192, or 256 bit keys. Designed as replacement for DES.
Agency - An organizational entity of the United States Federal Government. Also used in this document to refer to any entity authorized to purchase EIS services.
Agency Hierarchy Code (AHC) - A unique 28-character internal government accounting code that must be tracked for all services from order submission through disconnection.
Agency Locations - The physical address of agencies, sub-agencies, or other authorized users of EIS services.
Agency Service Request Number (ASRN) - Agency-provided service request number.
Alliance for Telecommunications Industry Solutions (ATIS) - A North American organization, formerly called ECSA, established to develop standards and guidelines for the methods and

procedures needed in the telecommunications industry. ATIS has four committees, T1, SONET, Internet Work Interoperability Test Coordination, and Order and Billing Form.
Alphanumeric - Any of the 26 upper-case alphabetic letters (A through Z) and 10 numerals only (0 through 9).
Alternate Mark Inversion (AMI) - A line coding method used in T-1 and other digital wire transmission systems.
American National Standards Institute (ANSI) - The US organization that sets the rules and procedures for, and also authorizes specific standards setting organizations. ATIS and EIA/TIA are two ANSI authorized standards setting organizations in the US in the subject area of telecommunications.
American Standard Code for Information Interchange (ASCII) - The standard code used for information interchange among data processing systems, data communications systems, and associated equipment in the United States.
Americans with Disabilities Act (ADA) - Public Law 101-336 (Public Law 336 of the 101st Congress), enacted July 26, 1990). The ADA prohibits discrimination and ensures equal opportunity for persons with disabilities in employment, State and local government services, public accommodations, commercial facilities, and transportation. It also mandates the establishment of TDD/telephone relay telecommunications services.
Application Programming Interface (API) - A software program that has defined information entry and exit points in that allows other programs or devices to communicate with the software program.
Associated Government Fee (AGF) Structure - The structure for calculating the AGF presented by GSA to the contractor (e.g., The AGF structure may be a fixed percentage of the billed eligible revenue).
Audio Conference - A feature that allows a call to be established among three or more stations in such a manner that each of the stations are able to carry on a communication with all the other stations.
Audit Trail - A record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.
Authentication - Verification of the identity of a user, device, or other entity in an IT system, often as a prerequisite to allowing access to resources in a system.
Authorization Code - An assigned code provided by the user to gain access to pre-subscribed EIS contractor-provided services and features.
Authorized User - An organization or user that is authorized to use the EIS contract and/or associated systems, including all Federal Agencies, authorized Federal contractors, agency-sponsored universities and laboratories, and when authorized by law or regulation, state, local, and tribal governments, and other organizations. All organizations listed in General Services Administration (GSA) Order OGP 4800.2I (as updated) are also eligible.

Automatic Call Distributor (ACD) - The device used by many offices to distribute incoming calls among employees; answers calls, determines how to handle the call, alerts the caller to remain on the line and then transfers the call to the first available employee

Automatic Message Accounting (AMA) - An automatic system for recording data describing the origination time of day, dialed number and time duration of a call for purposes of billing.

Automatic Number Identification (ANI) - A service feature in which the directory number or equipment number of a calling station is obtained automatically.

Automatic Protection Switching (APS) - Switching architecture designed for SONET to perform error protection and network management from any point on the signal path.

Automatic Switched Optical Network (ASON) - A multi-client versatile intelligent platform that enables automatic management of signaling and routing through a network. Enables policy-driven control of an optical network. Goal is a type of bandwidth on demand (BoD). Usually refers to Wide Area Networks (WANs)

Availability - Availability is the ratio of the time during which a service is available to the user (e.g., to originate and terminate calls) to the total amount of time in the calendar month. Availability is expressed as a decimal between 0 and 1, and is normally calculated for one calendar month of service.

Availability of Service - Defined as "The percentage of time a given service is available." Calculate as:

$$Availability(\%) = \frac{ElapsedTime - OutageTime}{ElapsedTime} \times 100$$

B Channel - The International Telegraph and Telephone Consultative Committee (CCITT) designation for a clear channel, 64 kb/s service capability provided to a subscriber under the Integrated Services Digital Network offering. (See Integrated Services Digital Network)

Bandwidth - The difference, in hertz (Hz), between the highest and lowest frequencies of a transmission channel. Also used to identify the maximum amount of data that can be sent through a given transmission channel per second.

Bare Metal Virtualized Servers – Servers running on "bare metal" or high-speed standardized generic hardware and using open-source software, as opposed to traditional servers that use proprietary hardware and software. "Virtualized" refers to their ability to be configured by software to look like servers running different operating systems or multiple instances of operating systems for different clients. The control software for these virtualized servers is usually called a "hypervisor."

Basic Rate Interface (BRI) - An Integrated Services Digital Network (ISDN) multipurpose user's interface standard that denotes the capability of simultaneous voice and data services provided over 2B+D channels, two clear 64 kb/s channels (B channels) and one clear 16 kb/s channel (D channel) access arrangement to each subscriber's location as defined by International Telecommunications Union/Telecommunications Service Sector (ITU-TSS) I.412. (See B Channel and D Channel)

Best Commercial Practice - That method(s), process(es), procedure(s), system(s), and/or usage that is commonly implemented in the business world and that is generally agreed to have produced the most satisfactory or desirable result(s) on a consistent basis.
Bidirectional Line Switched Ring (BLSR) - A form of synchronous optical network (SONET) transmission that uses 2 rings for communication. The data flow on these two rings is opposite: clockwise on one and counterclockwise on the other. The use of BLSR transmission allows half of the data communication devices to be served by one ring and half to be served by the other.
Bidirectional Path Switched Ring (BPSR) - SONET transport network configuration in which network nodes are connected in a ring and traffic can be instantly re-routed in the other direction around the ring in the event of a cable cut or degradation of optical signal, thereby routing around the point of failure.
Billed Price - Includes the actual price of equipment and/or services, AGF, and any billed charges that are defined in the EIS contract(s).
Billed Eligible Revenue - This represents revenue billed by the contractor that is included in the calculation of the Associated Government Fee (AGF) fee.
Billing Codes - These are specific alpha and/or numeric identifiers that are used in the contractor's commercial billing systems to represent various billing elements (e.g., feature charge type, transmission type, etc.).
Billing Dispute - A government notification to the contractor noting a difference between an actual invoiced amount and the correct amount, based on the contract.
Billing Inquiry - A question or issue in the area of billing which may lead to a billing dispute.
Billing Invoice – A contractor file produced not later than the 15th business day of every month containing all the chargeable elements of services delivered.
Billing Output files - This represents contractor output files related to contractual billing deliverables that are required by the government.
Bit - The smallest unit of data transmission, representing either a binary 1 or a 0.
Bit Error - An error in the transmission of a single bit.
Bit Error Rate (BER) - The number of bit errors divided by the total number of bits transmitted, received, or processed over some stipulated period.
Burst Size - The number of bytes that can be transmitted in a continuous stream.
Business Day - Any Monday through Friday that is not a US Federal holiday. *See also Government Business Day.*
Business Support System (BSS) - A system used to allow a network operator to perform the administrative portions of the business. These functions include billing, service ordering,

customer support, service management, inventory management, and program management. For purposes of this RFP, the definition includes all systems required to support the communications company including billing, service ordering, customer support, service management, inventory management, and program management.
Busy Hour Grade of Service (GOS) - Busy hour GOS is a KPI for VS and is defined as the proportion of calls that cannot be completed during the customer's busy hour because of limits in the call handling capacity of one or more network elements (e.g., all trunks busy). For example, P.01 GOS indicates that one percent of the calls attempted are not being completed during the busy hour.
Byte - A set of eight bits that represents a single unit.
Call Detail Records (CDR) - Network record (voice, data, or other) that includes call or event details, such as type, time, duration, originator, and destination; CDR may apply to network monitoring, traffic accounting, and billing.
Case Description - Contains sufficient information to distinguish one case from another of the same CLIN. This description will be used by the government agencies to assist in evaluation.
Channel Service Unit / Data Service Unit (CSU/DSU) - Devices that combine the functionality of data service units (DSU) and channel service units (CSU) to adapt data from user communication systems to service provider communication lines with multiple channels.
Circuit - The complete transmission path between two endpoints over which one-way or two-way communication may be provided. A circuit may provide one or more channels.
Circuit Emulation Services (CES) - A service that transports TDM-based traffic over a Metro Ethernet Network and looks to the user like a TDM circuit such as a T1.
Circuit Switched Data Service (CSDS) - Provides a synchronous, full duplex, totally digital, circuit-switched service at multiple data rates, including integral multiples of DS0 data rates (i.e., NxDS0, where N = 1 to 24) to on-net and off-net locations.
Circuit Switched Voice Service (CSVS) - Supports voice calls, whether initiated from on-net locations or from off-net locations after verification of authorization code, to be connected to all on-net and off-net locations by direct station-to-station dialing throughout the United States.
Class of Service (COS) - Classification of packets (or other transmission unit) for the purpose of treating certain classes or flows of packets in a particular way compared to other packets. For example, some classes may be expedited. Usually defined by specific service KPIs.
Classmark - A designator used to describe the service feature privileges, restrictions, and circuit characteristics for lines or trunks that access a switch.
Clear Channel - In networking, a signal path that provides its full bandwidth for a user's service. *Note:* No control or signaling is performed on this path (e.g., 64 kb/s clear channel).
Cloud - Set of servers and computers in a large installation accessed over the Internet or a private network capable of storing user data and/or downloading data and applications to user

devices. The cloud can also execute user programs and carry out other data processing functions.
Code Division Multiple Access (CDMA) - A system that allows multiple users to share one or more radio channels for service by adding a unique codes to each data signal being sent to and from each of the radio transceivers. These codes are used to spread the data signal to a bandwidth much wider than is necessary to transmit the data signal without the code.
Commercial Best Practice - Synonymous with "Best Commercial Practice"
Committed Burst Size (CBS) - The size up to which subscriber traffic is allowed to burst and still be in profile and not discarded.
Committed Information Rate (CIR) - A guaranteed minimum data transmission rate of service that will be available to the user through a network.
Common Language Location Identification Code (CLLI) - A location identification code that complies with American National Standard Institute (ANSI) standard T1.201-1987. The eight character mnemonic code is used to uniquely identify a location in the United States, Canada or other countries. These codes are known as CLLI or "Location Codes" and may be used in either a manual or mechanized record keeping system.
Compatibility - A property of systems that allows the exchange of necessary information directly and in usable form. *Note:* This implies use of identical or compatible protocols.
Competitive Local Exchange Carrier (CLEC) - A telephone service company that provides local telephone service that competes with the incumbent local exchange carrier (ILEC).
Computer Supported Telephony Applications (CSTA) - An interface created by ECMA to support computer telephony integration (CTI). ECMA is an industry association dedicated to the standardization of Information and Communication Technology (ICT) Systems.
Computer Telephony Integration (CTI) - CTI is the integration of computer processing systems with telephone technology.
Contract Line Item Number (CLIN) - A unique number used to identify billable items; a term used to describe an item that can have a single unit price; a contract line item must be identified separately from any other items or services on the contract.
CONUS - The 48 contiguous United States plus the District of Columbia.
Coordinated Universal Time (UTC) – A time standard commonly used across the world. .
Core Based Statistical Area (CBSA) - Metropolitan and Micropolitan geographic entities delineated by OMB for use in collecting, tabulating and publishing federal statistics (see OMB Bulletin No. 13-01, dated February 28, 2013).
Credit - An arrangement to reduce the amount owed by the customer on a future invoice by an agreed amount or for other Billing Adjustment (BA) reasons.

Critical Service Level - A level of service defined for government applications that specify higher levels of availability and performance than is assured by Routine Service.
Customer - Any entity included in OGP 4800.2I that purchases an EIS service or catalog item
Customer Network Management (CNM) - A data integration system that takes data from a service provider's fault, performance, and order management and provisioning systems, and integrates the data into a near real-time view for the enterprise customer.
Customer Network Management (CNM) Function - Provides an interface between users and the contractor's administrative and operational data, allowing users on-line access to "read" and download user's data while ensuring the service providers maintain information security and control.
Customer Relationship Management (CRM) - A process or system that coordinates information that is sent and received between contractors and customers. CRM systems are used to order, bill, to schedule activities, allocate resources, and help control the sales activities within a company.
Customer Support Office (CSO) - An organization which will be established by the contractor to provide direct, day-to-day customer service to the government. Also referred to as Customer Service Center (CSC).
Customer Want Date (CWD) - This represents the data by which the agency/customer desires to have service installed.
Cutover - The physical changing of circuits or lines at a telecommunications location after completion of service installations by a contractor.
D Channel - In ISDN, the 16 kb/s segment of a 144 kb/s, full-duplex subscriber service channel that is subdivided into 2B+D channels, i.e., into two 64 kb/s clear channels (B Channel) and one 16 kb/s channel (D Channel) for the ISDN basic rate.
Dark Fiber - Deployed fiber optic cable or cable strand that is not being used to transmit light waves. It is installed, but is not yet operational or has been taken out of service.
Data Dictionary - A set of information describing the contents, format, and structure of a database and the relationship between its elements.
Data Encryption Standard (DES) - A cryptographic algorithm for the protection of unclassified computer data, issued as Federal Information Processing Standard Publication 46-1. Obsolete, replaced by Advanced Encryption Standard (AES).
Data Integrity - The property that data meets a predefined level of quality or acceptability.
Decibel (dB) - A measurement of power increase or decrease based on taking the logarithm of the ratio of the power level being measured to a standard power level.
Dedicated Service Types - The access and transport service types generally based on the use of fixed transmission media and generally billed on a monthly recurring basis.

Dense Wavelength Division Multiplexing (DWDM) **-** A fiber-optic transmission technique that employs many closely-spaced light wavelengths to transmit data. Each light wave transmits a different data stream. ITU grid spacing for wavelengths in DWDM systems is 0.8 nm but is technically defined in terms of frequency (100 GHz).
Dialed Number Identification Service (DNIS) - A call identification service typically provided by a toll free (800 number) network. The DNIS information can be used by the PBX or automatic call delivery (ACD) system to select the menu choices, call routing, and customer service representative information display based on the incoming telephone number.
Digital Signature - A quantity associated with a message or file, e.g., a message digest encrypted with a private key, which only someone with access to a person's private key could have generated, but that can be verified through access and use of the associated public key. Usually considered as legally equivalent to a written signature.
Digital Subscriber Line (DSL) - A technology for transmission of digital information on a copper wire pair. Although the transmitted information is in digital form, the transmission medium is usually an analog carrier signal (or the combination of many analog carrier signals) that is modulated by the digital information signal.
Direct Billing - Agencies are invoiced directly by the contractor and pay the invoice directly to the contractor. The contractor is responsible for the collection of charges and AGF directly from the billed agencies or sub-agencies. GSA will not be responsible for any charges directly invoiced to any agency or sub-agency.
Direct Inward Dialing (DID) - Direct Inward Dialing (DID) connections are trunk-side (network side) end office connections. The network signaling on these 2-wire circuits is primarily limited to 1-way, incoming service. DID connections employ different supervision and address pulsing signals than dial lines. Typically, DID connections use a form of loop supervision called reverse battery, which is common for 1-way, trunk-side connections. Until recently, most DID trunks were equipped with either Dial Pulse (DP) or Dual Tone Multifrequency (DTMF) addresses pulsing.
Direct Ordering - A process in which agencies place orders directly with the contractor by using the contractor's ordering system or other processes agreed to by the parties
Direct-Billed Agency - A government agency or sub-agency that has elected to receive its billing directly from the contractor. Additionally, this represents a government agency or sub-agency that pays the contractor directly for services provided by the contractor.
Do Not Disturb (DND) - A term to describe a telephony feature that enables a user to temporarily block all calls to their telephone extension. DND provides the ability to temporarily block calls to a station number. The feature can be activated and de-activated by the subscriber. Outgoing calling capability is allowed when the DND state is activated. This capability can be administered on a station basis according to the subscribing agency's needs.
Domestic - Includes both CONUS and OCONUS regions
Dual-Tone Multifrequency Signaling - A telephone signaling method employing standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four relatively high frequencies.

Dynamic Allocation - A method for allocating charges among agencies in a shared tenant arrangement which applies to situations where the ANI is known for the agencies. *See Shared Tenant.*
E&M Signaling - In telephony, an arrangement that uses separate leads, called respectively the "E" lead and "M" lead, for signaling and supervisory purposes.
Effective Billing Date (EBD) - This represents the billing start date and may not precede the Service Order Completion Notice (SOCN) "complete date." Likewise, the billing end date must be the actual disconnect date indicated on the SOCN.
Electronic Access - The capability to access information via on-line access (dedicated or dial-up), electronic mail, and facsimile.
EDI – Electronic Data Interchange
EINSTEIN – See National Cyber Protection System
Electronic Fund Transfer (EFT) - Any transfer of funds, other than a transaction originated by cash, check, or similar paper instrument, that is initiated through an electronic terminal, telephone, computer, or magnetic tape, for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit an account. The term includes Automated Clearing House transfers, Fedwire transfers, and transfers made at automatic teller machines and point-of-sale terminals. For purposes of compliance with 31 U.S.C. 3332 and implementing regulations at 31 CFR part 208, the term "electronic funds transfer" includes a government-wide commercial purchase card transaction.
Electronic Mail (e-Mail) - A process of sending messages in electronic form. These messages are usually in text form. However, they can also include images and video clips
Emergency Change - Represents a change to an invoice's content or format that is required to occur prior to the minimum 60-day frequency.
Enclave - In this RFP, refers to Security Enclaves. A set of information and processing capabilities that are protected as a group. The information processing capabilities may include networks, hosts, or applications.
Encrypt - To convert plain text into an unintelligible form by means of a crypto system.
End of Unacceptable Service Performance - The time following the start of a period of unacceptable service performance at which time all KPIs once again meet or exceed their associated AQLs.
End-to-End - Telecommunications service from the originating user's terminal to the destination user's terminal. As applied in this document, this term refers to Service Delivery Point (SDP) to SDP service.
Enhanced 911 (E911) - An emergency telephone calling system that provides an emergency dispatcher with the address and number of the telephone when a user initiates a call for help. The E911 system has the capability of indicating the contact information for the local police, fire, and ambulance services that are within a customer's calling area.

Enterprise Infrastructure Solutions (EIS) - A comprehensive solution-based vehicle to address all aspects of federal agency information technology telecommunications, and infrastructure requirements.
Enterprise Infrastructure Solutions (EIS) Services - Services provided by the contractor to the customers under the EIS contract acquisition(s).
Envelope - In the context of message handling systems, as used in this document, envelope is an object that carries addressing information, and attributes (e.g., date, time, priority and subject) required for transporting the message.
Error Free Second (EFS) - A one second interval of digital signal transmission in which no transmission error occurs.
Errored Block - A data block in which one or more bits are in error.
Errored Second (ES) - A one-second interval of digital signal transmission in which at least one transmission error occurs.
Ethernet Private LAN (E-LAN) - A multi-point to multi-point service where disparate LAN segments are connected to form a single virtual LAN. Appropriate applications are inter and intra-city LAN connectivity, router interconnect and server consolidation. E-LAN can be offered over either a Metropolitan Area Network (MAN) or a Wide Area Network (WAN).
Ethernet Private Line (E-LINE) - A point-to-point service where bandwidth is reserved. E-LINE ES is useful for mission critical traffic. E-LINE resembles traditional Time Division Multiplexing (TDM) private line service. Appropriate applications are router interconnect, business continuity, and disaster recovery.
Exchange Rates - Shall be those in effect at close of business on the first working day of each billing period, as published by the Federal Reserve Statistical Release Foreign Exchange Rates Monthly Update or other mutually agreed source. No mark-ups or overhead charges shall be permitted on currency conversions.
Expedited Service Class A - The ordering agency requires priority provisioning for National Security / Emergency Preparedness (NS/EP) circumstances, or under circumstances in which the National Communications System (NCS) invokes the Telecommunications Service Priority (TSP) system. *See also Class A Expedited Implementation*
External Timing Reference (ETR) - Facilitates the synchronization of time-of-day (TOD) clocks to ensure consistent time stamp data in an installation with multiple, coupled systems.
Fail-Over Time - The time interval between the loss of a restorable network data link and its automatic restoration by imbedded management protocols.
Feature - An additional capability beyond basic service that is to be selected at the option of the user. Features are normally separately priced, although some features have been defined to be not separately priced.
Federal Acquisition Regulation (FAR) - The primary regulation for use by all Federal Executive Agencies in their acquisition of supplies and services with appropriated funds. It became

effective April 1, 1984 and is issued within applicable laws under the joint authorities of the Administrator of General Services, the Secretary of Defense, and the Administrator for the National Aeronautics and Space Administration, under the broad policy guidelines of the Administrator, Office of Federal Procurement Policy, Office of Management and Budget.
Federal Agency - In FAR definition, means any executive agency or any independent establishment in the legislative or judicial branch of the government (except the Senate, the House of Representatives, the Architect of the Capitol, and any activities under the Architect's direction).
Federal Communications Commission (FCC) - Federal Agency established by the Communication Act of 1934 that oversees commercial spectrum usage, interstate telecommunications, and all international services originating and terminating in the United States.
Federal Information Security Management Act (FISMA) - a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107–347, 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States.[1] The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
Federal Relay Service - A Federal Government-provided service that acts as an intermediary between hearing individuals and individuals who are deaf, hard of hearing, or have speech disabilities.
Federal Telecommunications Recommendations (FTR) – A set of telecommunications recommendations for the design and procurement of telecommunications equipment/services for the National Communications System (NCS). The FTR are issued by the NCS technology and program division, after approval by the FTR standards committee and deputy manager, NCS, pursuant to Executive Order 12472, Public Law 104-113 and NCS directive 4-1. *{Source: NCS web page}*
Fiber Connectivity (FICON) - An IO protocol used between IBM (and compatible) mainframes and storage. It takes the higher layer ESCON protocol, analogous to SCSI, and maps into onto a Fiber Channel transport.
File Transfer Protocol (FTP) - A Transmission Control Protocol/Internet Protocol (TCP/IP) service that supports bidirectional transfer of binary and ASCII files without loss of data between local and remote computers on the Internet. The FTP command set allows a user to log onto a remote server over the network, list file directories and copy files.
FIPS 140-2 Encryption – a U.S. government computer security standard used to accredit cryptographic modules.
Firewall - A system that manages a boundary between two networks to control access between the networks. A firewall as a single point of entry to an organization's intranet from the Internet provides a method for the security official to limit public access to data on an organization's intranet while allowing users on the intranet to access the WWW.
Firm Order Commitment Date – The date that the contractor commits to provide the service in a state ready for the customer to use and the date that the government expects to accept the

service and billing to become effective. It is the date specified on the Firm Order Commitment Notice in accordance with Section G.3.3 (Ordering Services).
Fraudulent Use of Services - Any use of EIS services for any functions or activities not authorized by the government.
Full-Duplex - A mode of operation in which simultaneous communication in both directions may occur between two terminals. Contrast with half duplex or simplex operation in which communications occur in only one direction at a time.
General Packet Radio Service (GPRS) - A portion of the GSM specification that allows packet radio service on the GSM system. The GPRS system adds (defines) new packet control channels and gateways to the GSM system.
Gigabit Ethernet (GigE) - Gigabit Ethernet (GE) is a data communication system that combines Ethernet technology with fiber optic cable transmission to provide data communication transmission at a Gigabit rate.
Gigabits per second (Gbps) – A measure of data transfer speed equal to one billion (10^9) bits per second.
Gigabyte (GB) – A measure of the size of binary data stored in memory or fixed media equal to 1,073,741,824 (2^{30}) bytes.
Gigahertz (GHz) - A measure of frequency equal to one billion (10^9) cycles per second. Signals operating above 1 GHz are commonly known as microwaves.
Government Data Elements - Data elements related to billing that are required by the government, and allows the government, at a minimum, to: • Verify information back to a service order, • Validate all charges, • Verify adjustments at the lowest level (e.g., service period of original charge type/description), • Enable the government to re-bill its own customers, • Assist with the management of inventory.
Government Fiscal Year – The 12-month period ending on 30 September of that year, having begun on 1 October of the previous calendar year
Government Furnished Equipment (GFE) - Property in the possession of, or directly acquired by the government and subsequently made available to the contractor. (See Government Furnished Property (GFP)
Government Furnished Property (GFP) - Property in the possession of, or directly acquired by the government and subsequently made available to the contractor.
Grade of Service (GOS) - A term associated with telecommunications service indicating the probability of a call being blocked during a call attempt during the busy hour, expressed as a decimal fraction.

Ground Start - A supervisory signal from a terminal to a switch in which one side of the line is temporarily grounded.
GSA Conexus - GSA's next-generation network solutions management system. This system is distinct from GSA Systems.
GSA Contracting Officer - The GSA contracting officer who administers EIS contracts.
GSA Systems - The set of tools used by GSA to manage the contract and TOs issued under the contract. These systems are distinct from GSA Conexus.
HyperText Markup Language (HTML) - Authoring software language used on the Internet and for creating WWW pages. HTML is essentially text with embedded HTML commands identified by angle brackets and known as HTML tags.
HyperText Transfer Protocol (HTTP) - The communications protocol used by a Web Browser to connect to Web servers on the Internet.
HyperText Transfer Protocol Secure (HTTPS) - The protocol for accessing a secure Web server. The use of HTTPS in the Uniform Resource Locator (URL) directs the message to a secure port address instead of the default Web port address of 80.
Identification (User ID) - The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.
Inbound - A switched connection made from a non-domestic location to a domestic location.
Indefeasible Rights of Use (IRU) - In telecommunications, Indefeasible Right of Use (IRU) is the effective long-term lease (temporary ownership) of a portion of the capacity of an international cable. This term is used in Dark Fiber Services.
Individual Case Basis (ICB) – Applies to a situation with special end-user requirements, for which special arrangements are made with the contractor where fixed pricing could not have been determined or could not apply.
Infrastructure as a Service (IaaS) – Cloud-based offering in which user gains access to virtual machines, servers, storage, and other infrastructure for the purpose of implementing a data center, for system testing, or other purpose. Users typically install their own images or operating systems on the cloud infrastructure.
Institute of Electrical and Electronics Engineers (IEEE) - An organization formed in 1963 that represents of electrical and electronics scientists and engineers.
Integrated Services Digital Network (ISDN) - A service that provides end-to-end digital connectivity to support a wide range of services, including voice and non-voice services, to which users have access by a limited set of standard multi-purpose user network interfaces, as defined in the ITU-TSS I series. (See basic rate interface and primary rate interface.)
Interactive Voice Response (IVR) - IVR is a process of automatically interacting with a caller through providing audio prompts to request information and store responses from the caller. The

responses can be in the form of touch-tone(tm) key presses or voice responses. Voice responses are converted to digital information by voice recognition signal processing.
Interconnection - The linking together of interoperable systems.
Inter-exchange Carrier (IXC) - Also known as long distance carriers, inter-exchange carriers (IXCs) interconnect local systems with each other. For inter-exchange connection, networks as a rule connect to long distance networks through a separate toll center (tandem switch). In the United States, this toll center is called a point of presence (POP) connection.
Intermediate Reach – Single – Longitudinal Mode (IR1-SLM) - Intermediate Reach (IR) optical interfaces refer to optical sections with system loss budgets from 0 dB to 11 or 12 dB. Typically, low power SLM or MLM laser transmitters are used at the lower bit-rates, while high-power SLM lasers are used at the higher bit-rates.
International Telecommunications Union (ITU) – see "Consultative Committee for International Telephony And Telegraphy (CCITT)"
Internet - A worldwide interconnection of individual networks operated by government, industry, academia, and private parties.
Internetworking - The process of interconnecting a number of individual networks to provide a path from a terminal or a host on one network to a terminal or a host on another network. The networks involved may be of the same type, or they may be of different types. However, each network is distinct, with its own addresses, internal protocols, access methods, and administration.
Interoperability - The ability of systems to provide services to and accept services from other systems and to cause services from different systems to operate effectively together so as to achieve the throughput and service quality (i.e., required grade-of-service, transmission quality, and feature capability) that is agreed to be acceptable. The condition achieved among telecommunication systems when information or services can be exchanged directly and satisfactorily between them and/or their users. Interface devices or gateways may be placed between equipment or systems in order to achieve interoperability.
Inventory Reconciliation (IR) – Deliverable document that compares delivered service to ordered services and lists discrepancies.
Invoicing - The process of preparing and forwarding a list of charges to the government for services rendered by the contractor.
IP-Security (IPsec) – A group of IP security measures which together comprise a highly secure tunneling protocol for IP communications.
IS-41 – Intersystem Signaling, also known as ANSI-41. Mobile cellular telecommunications system standard to support networking of switches. Facilitates inter-switch operations such as call handoff and roaming authentication.
Jitter - Jitter, also known as cell delay variation or packet delay variation, is a measure of the variance of cell or packet transfer delay. High variation implies the need for larger buffering for delay-sensitive traffic such as voice and video. Jitter is caused by several factors that combine to

cause packet delay variation, including variations in the propagation delay, queuing delays at various intermediate switches, and service times at switching points.
Key Performance Indicator (KPI) - A measurable service attribute that is critical to the proper functioning and delivery of a telecommunications service. KPI types are listed in Sec. C.1.8.3. Each EIS service is associated with KPIs that are specified in Section C.2 (Technical Requirements).
Kilobits per second (Kbps) – A measure of data transfer speed equal to one thousand (10^3) bits per second.
Kilobyte (KB) – A measure of the size of binary data stored in memory or fixed media equal to 1,024 (2^{10}) bytes.
Kilohertz (KHz) - A measure of frequency equal to one thousand (10^3) cycles per second.
Last Number Dialed (LND) – A term to describe a telephony feature that enables a telephone device to dial the most recently dialed telephone number.
Latency – Also known as cell latency, cell transfer delay, or packet transfer delay, it is the round-trip delay between transmission and receipt of a packet measured between network access points. Normally latency is expressed in milliseconds and the rate of delay is sampled over a brief period, typically one minute or less, to arrive at an average latency figure. Latency includes propagation delays, queuing delays at various intermediate components such as routers and switches, and service times at switching and routing points.
Layer 2 Tunneling Protocol (L2TP) - A protocol that is used to allow a secure communication path, a virtual private network link, between computers. It is an evolution of earlier point-to-point tunneling protocol (PTPP) as it offers more reliable operation and enhanced security. L2TP enables private communication lines through a public network. L2TP was developed via the Internet Engineering Task Force (IETF).
Layer 3 – The network layer in the Open Standards Interconnection Model (OSI). Layer 3 protocols handle routing within and between networks.
Link Capacity Adjustment Scheme (LCAS) - SONET term referring to a portion of the overhead in a SONET frame.
Local Area Network (LAN) - A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. .
Local Exchange Routing Guide (LERG) – A Telcordia publication that relates Numbering Plan Area (NPA)/NXX to the Vertical and Horizontal (V&H) and CLLI Code of the associated wire center.
Local Government Contact (LGC) – An individual designated by a CO on a service request to interface with the contractor at a specific agency location on his behalf. LGC participates in service transition planning and implementation activities for a location, however, the decision to change or modify a service order placed by the CO or COR, remains with the CO or COR.

Local Number Portability (LNP) - LNP is the process that allows a subscriber to keep their telephone number when they change service provider in their same geographic area. Local number portability requires that carriers release their control of one of their assigned telephone numbers so customers can transfer to a competitive provider without having to change their telephone number. LNP also involves providing access to databases of telephone numbers to competing companies that allow them to determine the destination of telephone calls delivered to a local service area.
Location – In this document, is a physical place where (1) a user of EIS services resides or (2) telecommunications services are available or (3) EIS services are delivered. Also construed to include wireless terminals. *(See Agency locations, SDP locations, PSTN locations)*
Long Haul (LH) – A communication system which includes a number of drop/add points, repeaters locations, over long distances that extend outside the local service area; a microwave system that the longest radio circuit of tandem radio paths exceeds 402 km (250 miles).
Loss - The amount of electrical attenuation in a circuit, or the power consumed in a circuit component.
Management Information Base (MIB) - In Simple Network Management Protocol (SNMP), the set of information about a managed object used by the management program.
Mandatory – These are services, features, or equipment which the contractor must propose. Any mandatory service, feature or equipment proposed must be priced.
Mapping - In Electronic Data Interchange (EDI), mapping refers to a defined process to translate a company's proprietary data layout to an interoperable EDI format.
Mean Opinion Score (MOS) - In voice communications, particularly Internet telephony, the mean opinion score (MOS) provides a numerical measure of the quality of human speech at the destination end of the circuit. The scheme uses subjective tests (opinionated scores) that are mathematically averaged to obtain a quantitative indicator of the system performance.
Meet-Me Conference - Allows stations to be connected in a conference by dialing one access code at a particular time.
Megabits per second (Mbps) – A measure of data transfer speed equal to one million (10^6) bits per second.
Megabyte (MB) – A measure of the size of binary data stored in memory or fixed media equal to 1,048,576 (2^{20}) bytes.
Megahertz (MHz) - A measure of frequency equal to one million (10^6) cycles per second.
Minimum Point of Penetration (MPOP) - An FCC defined location in a building/premises where an SDP is located normally.
Mobile Satellite Service (MSS) - A form of wireless service that employs satellites as part of the wireless infrastructure and is capable of serving very large geographic areas. The use of MSS may be appropriate for areas that are economically not viable for land based radio towers or to provide wide area group call (dispatch type) services**.**

Monthly Billing Informational Memorandum - A report provided by the contractor to the government which includes, but is not limited to, items that will explain changes in billing, changes to data formats, new services added to the billing, and issues pertaining to balancing charges.
Monthly Recurring Charge (MRC) - A fixed charge paid monthly
Multi-Line Key Telephone Systems - Telephone station equipment conforming to the Electronic Industries Association (EIA) standard RS-478, first published in July 1981.
Multimedia - Pertaining to the processing and integrated presentation of information in more than one form, e.g., video, voice, music, data.
Multi-Mode Fiber (MMF) – Optical fiber that is designed to carry multiple light rays or modes of light concurrently, each at a slightly different reflection angle within the optical fiber core, that is used for relatively short distances. Differs from Single Mode Fiber (SMF) because it has a larger core (usually 50 or 60 micrometers compared to 9 micrometers).
Multiprotocol Label Switching (MPLS) - A network routing protocol based on switching packets through a network by the use of tag labels, instead of routing them. Since switching is much faster than routing, this method can speed up network performance. .
National Agency Check - The computerized search of the National Crime Information Center computer network of various government (state, local, Federal, and tribal) agencies.
National Cyber Protection System (NCPS), also known as EINSTEIN – Deep packet inspection system designed to look for malware in packets traversing the Internet and destined for delivery to a government agency.
National Security and Emergency Preparedness Requirements (NS/EP) - Requirements for capabilities that maintain a state of readiness or respond to and manage an event or crisis (local, national, or international), which causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security and emergency preparedness posture of the U.S. EIS NS/EP requirements are consistent with guidance from the DHS Office of Emergency Communications.
National Telecommunications and Information Administration (NTIA) - A policy unit of the Department of Commerce which assigns frequencies in the spectrum used by the federal government. The NTIA also advises the President and Congress on telecommunications issues.
National Telecommunications Management Structure (NTMS) - NTMS is a principal Government Emergency Telecommunications Service (GETS) supported functions for providing network management during national emergency.
National Television Standards Committee (NTSC) Standard - The North American standard (525-line interlaced raster-scanned video) for the generation, transmission, and reception of analog television signals. Now largely obsolete because of new digital video standards such as High-Definition (HD) television.

Network Entry Point - A system that receives ANSI X12 Electronic Data Interchange transactions and transfers them to Value Added Networks. A Network Entry Point can provide services such as archival, date and time stamp, file transfer, and access to other networks such as the Internet.
Network Functions Virtualization (NFV) - the virtualization of network equipment functions, which typically run on dedicated appliances, to now run on industry-standard servers, switches and storage devices with the aim of lowering costs, improving efficiency and increasing agility.
Network Site Code (NSC) - Identifies a physical location, a customer agency building, Physical Concentration Location, and/or Point of Presence. See Section B.4.1 for details.
Node - Center for the interconnection of two or more branches of a telecommunications network.
Non-Domestic - The worldwide countries and locations other than those defined herein as domestic.
Non-recurring Charge (NRC) - A cost for a facility, service, or product that only occurs one time or is not periodically charged.
North American Numbering Plan (NANP) – The numbering system that creates unique phone numbers for network dialing in the US, Canada, and some Caribbean islands; a numbering plan which allows all stations conforming to the 10-digit dialing pattern of the Public Switched Network (PSN) to be accessed. The pattern is of the form NPA-NXX-XXXX where NPA= (Area Code); N = 2-9; P = 0-9; A = 0-9; and X = 0-9. The NANP is a subset of and consistent in format with the ITU/TSS ISDN E.164 Uniform numbering and addressing plan used worldwide.
North American Standard for Wireless Telecommunications Network Signaling (IS-41) – See "Intersystem Signaling 41 (IS-41)"
Not Separately Priced (NSP) - A capability or feature that is included in the price of the basic service.
Notification of Data File Loading Problems - An email notification provided by the GSA to the contractor intended to alert the contractor of system file loading problems associated with the media or data the contractor provided.
Numbering Plan Area (NPA) – The first three digits of a North American telephone number, often called an area code, in which the first digit cannot be a 1 or a 0 and that the remaining numbers can be 2 through 9.
OCONUS - U.S. territories and possessions outside of the contiguous 48 states. It includes Alaska, Hawaii, Guam, Puerto Rico, US Virgin Islands, Marshall Islands, Midway Island, Palau, Wake Island, American Samoa, Commonwealth of Northern Marianas Islands (CNMI) and Micronesia
Office of Emergency Communication (OEC) – The mission of the OEC is to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget in (1) the exercise of the telecommunications functions and responsibilities, and (2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack & recovery

and reconstitution. {source *www.NCS.gov* website}. Formerly known as the National Communications System.
Official List Price (OLP) - Term defined under EIS to include a variety of possible list price types. For example, if the catalog item is equipment not manufactured by the contractor, the OLP could be the Original Equipment Manufacturer's Published List Price. When the catalog item is a service provided by the contractor, the OLP could be the contractor's Published List Price for the service.
Official Manufacturer's List Price – The manufacturer's list price for a SRE as found on an up-to-date document containing undiscounted list price information that is provided to a lessor or reseller of the SRE by the manufacturer, and that can be confirmed by similar documents provided by the manufacturer to other equipment or service providers or is available on its website.
Off-Net Call - A call between two or more stations, at least one of which is a presubscribed user or service delivery point (usually a PBX or Centrex) and at least one of which is not.
Off-Net Location – A location that is not presubscribed to services provided by EIS, i.e., a location "off" of the EIS network. Certain EIS services can transmit and receive communications with locations not "on" the EIS network, such as commercial telephone lines on the PSTN and personal computers connected to the Internet.
On-Net Call - A call between two or more on-net locations.
On-Net Location - A location that is presubscribed to services provided by an EIS contractor, i.e., a location "on" the contractor's EIS network. On-net locations may be implemented using either dedicated access or a presubscribed switched access arrangement. On-net locations shall be construed to include presubscribed terrestrial and satellite service-based wireless handsets or terminals.
Optical Add-Drop Multiplexer (OADM) – A network element that allows the extraction/insertion of one or more wavelengths from/to the multi-wavelength signal as it is passed through the element.
Optical Carrier Hierarchy Level-N (OC-n) – In SONET systems, Optical carrier (OC-n) transmission is a hierarchy of optical communication channels and lines that range from 51 Mbps to 40 Gbps . The "n" is an integer (typically 1, 3, 12, 48, 192, or 768) representing the data rate.
Optical Transport Network (OTN) – Replacement for SONET that will do SONET functions such a framing in a manner more suited to faster provisioning and network flexibility. Designed to interface between Wave Division Multiplexing (WDM) equipment and higher layers in OSI protocol stack. Consists of six layers, of which Optical Transport Unit (OTU) and Optical Channel (OCh) are most commonly referred to.
Optical Wavelength Service (OWS) - Provides connectivity to data centers, carrier hotels, and enterprise businesses and tremendous bandwidth capacity of a dedicated wavelength connection, without the significant upfront capital costs or the management and maintenance issues associated with a dark fiber network.

Optional – Those services, features, or equipment which contractors may propose but are not required to propose. Any service, feature or equipment proposed must be priced.
Optronics – The combination of optical and electronic functions in one piece of telecommunications equipment that provide an interface between electrical and optical telecommunications modes.
Outage - A telecommunication service condition wherein a user is deprived of service due to a malfunction of the contractor's communication system.
Outbound - A switched connection made from a domestic location to a non-domestic location.
Password - A word, character, or combination of characters that permits access to otherwise inaccessible data, information, or facilities. Also referred to in this document as an authorization code.
Past Performance Information Retrieval System (PPIRS) - A database retrieval system utilized by the Contracting Officer (and Ordering Contracting Officer) in assessing past performance of contractors. In conformance with the government's need to record and maintain information on contractor performance during the life of this contract, the government periodically evaluates the manner in which the contractor performed in accordance with contract requirements such as: quality of service; cost efficiencies; timeliness; business relations; history of reasonable and cooperative behavior; commitment to customer satisfaction; and key personnel.
Payload - In a set of data, such as a data field, block, or stream, being processed or transported, the part that represents user information and user overhead information, and may include user-requested additional information, such as network management and accounting information. Note: The payload does not include system overhead information for the processing or transportation system.
Performance-based Contracting – In FAR definition, means structuring all aspects of an acquisition around the purpose of the work to be performed with the contract requirements set forth in clear, specific, and objective terms with measurable outcomes as opposed to either the manner by which the work is to be performed or broad and imprecise statements of work.
Period of Unacceptable Service Performance - Period of time during which the service provided is incapable of supporting one or more of the customer's uses or applications that normally would be supported by the service. The start and end of a period of unacceptable service performance may be reported either by the contractor or by the customer. *See Unacceptable Service Performance.*
Platform as a Service (PaaS) – Cloud-based offering in which providers deliver a computing platform, usually including operating system, programming-language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. In some cases resources are scaled automatically in response to user needs.

PMM (Price Management Mechanism) Demand Set - A statistically significant traffic set extracted from the contractor's EIS usage for each of the services subject to the PMM process and for the contract period under review by the PMM process.
Physical Concentration Location (PCL) - Any place where connections are aggregated. See Section B.4.1 for details.
Point of Presence (POP) – A contractor-owned or controlled physical location where network facilities provide EIS services and where user agency locations are connected to the network. See Section B.4.1 for details.
Polarization Mode Dispersion (PMD) - In single mode fiber optic cable, refers to the fact that the two orthogonal polarizations of light waves in the core travel at slightly different speeds, leading to slow smearing of pulses as they traverse the fiber. PMD can limit the highest bit rate that is achievable in a fiber optic system.
Post Office Protocol Version 3 (POP3) –Post Office Protocol version 3. A protocol used to retrieve e-mail from an e-mail server. POP3 is described in detail in IETF RFC 1939.
Preset Conference - A feature that allows designated users to establish a conference by dialing a single number.
Price Management Mechanism (PMM) - A special contract requirement establishing a process to ensure that EIS service prices remain competitive with prices paid by other large users of telecommunications services. The competitiveness of EIS service prices is examined by comparing the cost when EIS prices are applied to demand sets with the cost when pricing from comparison commercial and other government contracts, price schedules, and tariffs are applied to the same demand set. Reductions in EIS contractor prices will be required if a lower comparison cost is found through the PMM process.
Pricing Hub (PHub) - Used to assign a unique identifier to locations with the same price for the same access service type. See Section B.4.1 for details.
Primary Inter-exchange Carrier (PIC) - Refers to the company that is selected by the subscriber to be its main long distance company. It is the carrier chosen by a subscriber to be accessible via simplified dialing pattern.
Primary Rate Interface (PRI) - An ISDN interface standard that is designated in North America as having a 23B+D channels. (See Integrated Services Digital Network)
Prime Contract - A contract or contractual action entered into by the U.S. for the purpose of obtaining supplies, materials, equipment, or services of any kind.
Prime Contractor - A corporation, partnership, business association of any kind, trust, joint-stock company, or an individual who has entered into a prime contract with the U.S.
Private Branch Exchange (PBX) - Telephone switching equipment designed to allow a large number of telephones in an office to call each other, and share one or more outside lines to connect to the PSTN. Conforms to the EIA standards RS-464 and RS-464-1, published in December

1977 and August 1982, and meeting Federal Communications Commission (FCC) registration requirements for interconnection to the public switched network.
Private Line Service (PLS) - The service category covering provision of private-line transmission of voice or data using end-to-end transmission media. (See Dedicated Transmission Service)
Program Management Office (PMO) - An office within the GSA/FAS organization responsible for management and contract administration of a telecommunications program. Within the context of this document, it refers to the specific PMO responsible for the EIS program.
Project – A project requires special treatment by the contractor due to the size, complexity, or importance of the services ordered as a project. The customer may request that the order be implemented as a project. In such cases, the contractor shall develop a Task Order Project Plan. Provisioning intervals will be as agreed to between the contractor and the ordering agency.
Project Identifier - A Project Identifier is a code or number assigned by the contractor or government and shown by the contractor on a series of service orders to identify each service order that is part of a larger group in progress.
Project Service Request - Multiple requests for service that are associated with a particular project and are related in such a manner that they should be implemented in a coordinated fashion.
Prompt Payment Clock - This represents the date and time, or the period of time from which the government has received all monthly billing deliverables as required by the contract until the payment has been made by the government to the contractor. GSA will start the Prompt Payment clock according to FAR Clause 52.232-25 when the detail billing has been delivered to the government (See Section G.4 Billing).
Public Safety Answering Point (PSAP) – A physical location where 911 emergency telephone calls are received and then routed to the proper emergency service.
Public Switched Telephone Network (PSTN) – Common domestic telecommunications network that interconnects private branch exchange trunks, telephones, Centrex systems, and wireless terminals and handsets.
Quality of Service (QoS) – User's experience over a network connection. Usually measured by a defined set of engineering values for a service that is guaranteed by the contractor Typical QoS parameters are bandwidth, delay or latency, jitter, packet loss, and out-of-order delivery.
Radio Frequency (RF) - Those frequencies of the electromagnetic spectrum normally associated with radio wave propagation. RF sometimes is defined as transmission at any frequency at which coherent electromagnetic energy radiation is possible, usually above 150kHz.
Relay Service – *See Federal Relay Service*
Role Based Access Control (RBAC) – Allows only authorized users with appropriate permissions access to the BSS.
Routine Order – An order for which the contractor's standard provisioning interval applies.

Routine Service Level – A level of service that applies for most government applications and is expected to reflect commercial best practices for service availability and performance.
Satellite Internet Service (SIS) – Provides Internet access through satellite communications. This is mostly applicable to small rural sites without broadband wireline or wireless access or that need a backup Internet connection, and sites that require backup communications during a national emergency or disaster.
Sawtooth Effect – In this RFP, the effect observed when using declining unit prices in a set of increasing dollar ranges to determine a cost associated with a particular range. The cost is determined such that the last cost within a lower dollar range is higher than the first cost within the next higher dollar range, and the first cost within the next dollar range is lower than the last cost within the previous dollar range.
SDP Locations – *See Service Delivery Point (SDP)*
Secured E-Mail - Process by which electronic documents, reports, or files are provided or delivered to the government via E-Mail in a secured manner (e.g., E-Mail over a private network, encrypted E-Mail, encrypted attachment in an E-Mail).
Secured FTP Media - Distribution media by which electronic documents, reports, or files are provided or delivered to the government via File Transfer Protocol (FTP) server in a secured manner (e.g., SFTP, FTP over a Virtual Private Network, and FTP over a private network).
Secured Web-based Media - Distribution media by which electronic documents, reports, or files are provided or delivered to the government via a HTTP server in a secured manner (e.g., HTTPS, HTTP over a Virtual Private Network, and HTTP over a private network).
Security Violation - Any unauthorized action taken by any domestic or international party (contractor employee or non-employee) that: a) violates contractor's security policies, b) bypasses contractor's security mechanisms, C) gains unauthorized access to contractor's facilities, information, information systems, or management systems, d) intentionally affects the quality, integrity, or availability of services offered to the government, e) alters or destroys any EIS services information held by the contractor and/or provided to the government, f) discloses confidential or secret information, and/or g) compromises national security.
Service - The term "Service" refers to the primary unit of EIS technical and pricing requirements. It includes all components and functions provided by the contractor to deliver a specific service, including the contractor's network, contractor-provided access arrangements and service related equipment. Individual services are grouped into "Service Types." *Also see "Service Types"*
Service Access Code (SAC) - The 3-digit codes in the NPA (N 0/1 X) format which are used as the first three digits of a 10-digit address in a North American Numbering Plan dialing sequence. Although NPA codes are normally used for the purpose of identifying specific geographical areas, certain of these NPA codes have been allocated to identifying generic services or to provide access capability, and these are known as SACs. The common trait, which is in contrast to an NPA code, is that SACs are non-geographic.

Service Delivery – A process which begins at the time an order is accepted by the contractor and ends at the time service is accepted by the customer. Service delivery includes service provisioning and service acceptance sub-processes.
Service Delivery Point (SDP) - the interface point at which a service is delivered by the contractor to the government or its designated agent. The SDP is the interface point for the physical or logical delivery of a service, the point at which performance parameters are measured to determine compliance with the contract, and the point used by the contractor to identify the pricing for services rendered.
Service Level Agreement (SLA) - An agreement between the government and the contractor to provide a service at a performance level that meets or exceeds the specified performance objective(s). The contract has specific KPIs for nearly all services. If a contractor does offer a service, it must comply with those KPIs. For each KPI, the contractor shall meet specified Acceptable Quality Levels (AQLs). Certain services are deemed sufficiently essential to government operations to also require mandatory Service Level Agreements (SLAs). If the specified service levels are not met, then the contractor shall issue specified credits.
Service Level Agreement Credit Request (SLACR) – Request for credit submitted to a vendor when one of the vendor's services has failed to meet the performance criteria specified in the associated Service Level Agreement.
Service Related Equipment (SRE) – Contractor-provided equipment (composed of one or more devices) used to meet the User to Network Interface (UNI) requirements for an individual service and/or to implement access aggregation and integration to provide a lower service delivery cost to the government. SRE is also contractor-provided equipment used to enable the requirements associated with the Management and Applications Services and Security Services. In this RFP, SRE will be offered only as needed to provide delivery of a service procured under an EIS contract.
Service Order - The documentation that contains all information required to obtain a service. Service orders can be placed against a TO. The service order functional requirements and ordering procedures include the submission of service orders by agencies and the receipt of notifications from the contractor at appropriate points in the ordering interval, service delivery and fulfillment process.
Service Order Acknowledgement (SOA) - The acknowledgement provided by a service provider (contractor) that an order has been received from the ordering agency.
Service Order Completion Notice (SOCN) - The notice that contains data elements notifying the agency that the service for a given order has been fully installed and is ready for acceptance.
Service Order Confirmation (SOC) - The notice a contractor provides the agency that contains the data elements that a service for a given order is accepted as a valid service with all the information needed to start service provisioning.
Service Outage – Either a complete loss of service or degradation of service that is so severe that it is not able to support a customer application. A service outage that is reported to the contractor as an out of service (OOS) condition must be documented by a trouble ticket. Any service outage automatically causes unacceptable service performance, as defined below.

Service Restoration – The point in time at which the contractor returns service to a condition in which all KPIs meet or exceed their associated AQLs following the opening of a trouble ticket for either unacceptable service performance or for a service outage.
Service Restoration Time – The interval of time between the opening of a trouble ticket for either a service outage or for unacceptable service performance and service restoration.
Service Type – Describe a group of individual services that are similar and are grouped to simplify specification, offering and evaluation processes. Within each Service Type, individual services are specified. In EIS, there are twelve (12) Service Types as follows: 1. *Data Service*. Includes services such as VPNS, Ethernet, Optical Wavelength Service, Private Line, SONET, Dark Fiber and Internet Protocol Service 2. *Voice Service*. Includes services such as IPVS, CSVS, Toll Free and CSDS. 3. *Contact Center Service*. 4. *Colocated Hosting Service*. 5. *Cloud Service*. Includes services such as Infrastructure as a Service, Platform as a Service, Software as a Service, Content Delivery Network Services. *6. Wireless Service* *7. Commercial Satellite Service* 8. *Managed Services*. Includes services such as Managed Network Service, Web Conferencing Service, Unified Communication Service, Integrated Performance Monitoring Service, MTIPS, Managed Security Services, Managed Mobility Service, Audio Conferencing, Video Teleconferencing and Intrusion Prevention Security Service. *9. Access Arrangements* *10. Service Related Equipment* *11. Service Related Labor* *12. Cable and Wiring*
Serving Wire Center (SWC) – The wire center (also called a central office) from which the user agency's premises would normally obtain dial tone from its Local Exchange Carrier; the wire center from which dial tone service is provided to a local exchange service customer.
Session Initiation Protocol (SIP) - In VoIP systems, a protocol used for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging over Internet Protocol (IP) networks.
Severely Error Second (SES) – A one second interval of digital signal transmission in which 30% or more of the data stream contains errors. The occurrence of 10 or more contiguous severely error seconds on a Private Line Service data circuit causes service unavailability.
Simplex Operation - That mode of operation in which communication between two points occurs in only one direction at a time. Contrast with half duplex or duplex operation.
Single-Mode Fiber (SMF) – Optical fiber that is designed for the transmission of a single ray or mode of light as a carrier and is used for long-distance signal transmission. Has a smaller core than multi-mode fiber (9 micrometers vs 50 or 60 micrometers).
Software as a Service – Cloud-based offering in which providers manage infrastructure and platforms that run user-facing applications. Users access the applications from clients, often web-based

clients. Applications may maintain user account information and store user data in the cloud. Typical examples include e-mail and banking.
Software Defined Networking (SDN) -An approach to networking in which control is decoupled from the physical infrastructure, allowing network administrators to manage a network fabric across multi-vendor equipment by use of control planes and virtualization.
Specification - A document that clearly and accurately describes the essential technical requirements for items, materials, or services, including performance requirements.
Standard Features - Capabilities included with a service that are not separately priced (NSP) and are typically not separately identified. If a standard feature is identified by a separate CLIN, its price shall be zero. Standard features are service dependent.
Start of Unacceptable Service Performance – The time at which any of the KPIs for the service begins to fail to meet its associated AQL. This may be documented from the contractor's monthly performance report or from a trouble ticket initiated by the customer or the contractor.
Sub-Agency - A subsidiary billing entity as defined by the parent agency and identified by an Agency Hierarchy Code.
Synchronous Digital Hierarchy (SDH) - The International Telecommunications Union standard for fiber optic synchronous transmission rates which begins at 155 Mbps. SONET is a subset of SDH, and for most applications is functionally the same at OC-3 and higher rates.
Synchronous Optical Network Services (SONET) – Layer 2 technology for transmitting digital data over optical fiber with high reliability and low error rates. Subset of SDH.
Tariff – Document filed by a regulated telephone company with a state public utility commission or the Federal Communications Commission. The tariff is a public document that details services, equipment and pricing offered by the telephone company to all potential customers.
Task Order- An order for services that contains all of the information required in FAR 16.505.
Telecommunications Device for the Deaf/Teletypewriter (TDD/TTY) - A device that permits individuals with speech and/or hearing impairments to make and receive telephone calls without assistance from others. A TDD or TDD-compatible device will be used by the speech/hearing-impaired user community to access the Federal Relay Service. A TDD generally consists of a keyboard, display screen, and a means (via modem or direct connection) to access a telecommunications network. It is recognized that this function can be performed by a computer with software enhancements. The term TTY may also be used in referring to this type of device.
Telecommunications Services - The services and solutions that deliver or augment communications between users. It refers to a communications service or solution specified as a discrete offering or set of capabilities.
Telecommunications Service Priority (TSP) - The TSP program provides a framework for telecommunications services vendors to initiate, restore, or otherwise act on a priority basis to ensure effective NS/EP telecommunications services during national emergency. The TSP

System applies to common carriers, to government, and to private systems that interconnect with commercially provided services or facilities.
Terabyte (TB) – A measure of the size of binary data stored in memory or fixed media equal to 1,099,511,627,776 (2^{40}) bytes.
Time to Restore (TTR) - The Time to Restore (TTR) SLA measures contractor performance on a per-incident basis. The contractor shall calculate the TTR using the following method: 1. Find the elapsed time between the time a service outage is recorded in the trouble ticketing system and the time the service is restored. 2. Subtract time for any scheduled network configuration change or planned maintenance. 3. Subtract time, as agreed to by the government, that the service restoration of the service cannot be worked on due to government-caused delays. Examples of government-caused delays include: a) The customer was not available to allow the contractor to access the Service Delivery Point or other customer-controlled space or interface; b) The customer failed to inform the contractor that a security clearance was required to access the SDP or customer-controlled space; or c) The government required service at a remote site and agreed that a longer transit time was required.
Transfer "off" - The transfer of service from the contract to a follow-on contract or service arrangement, managed by GSA in a coordinated way to prepare for the expiration of the contract.
Transfer "on" - The transfer of service from an EIS contract or a GSA local services agreement (LSA) to the contract
Traffic Model - A representation of traffic. A model of 5-year estimated traffic to be used in preparation and evaluation of the EIS price proposals.
Transition - The process for the coordinated transfer of service from a specified GSA incumbent contractor to a new EIS contractor.
Transport - The facility-based service arrangements that provide service specific connections between the contractors' POPs.
Trouble Ticket – The method used by the contractor to record a service trouble either detected by the contractor or reported by the customer to the contractor. It is the primary method used by the government and the contractor to report and track a service outage or for unacceptable service performance.
Unacceptable Service Performance – A period during which the service provided is not capable of properly supporting the customer's intended application or use. Unacceptable service performance is caused by the failure of any combination of the key performance indicators (KPIs) to meet their specified acceptable quality levels (AQLs). Unacceptable service performance may or may not result in a service outage depending on the severity of service degradation; i.e., the amount by which the KPIs fail to meet their AQLs.

Uninterruptible Power Supplies (UPS) - An Uninterruptible Power Supply is a device that sits between a power supply (e.g. a wall outlet) and a device (e.g. a computer) to prevent undesired features of the power source (outages, sags, surges, bad harmonics, etc.) from adversely affecting the performance of the device.
Unique Billing Identifier (UBI) – The Unique Billing Identifier (UBI) is a contractor-assigned code that uniquely identifies a group of services that are related for ordering, billing and inventory purposes as well as uniquely identifying each component within that grouping.
User - An individual or agency that utilizes EIS services. *Also see Authorized User.*
User-to-Network Interface (UNI) – The specification of the physical, electrical, and signaling/protocol interface at the SDP for a specific information payload bandwidth or data transfer rate for interconnection of user equipment to an access segment.
Vertical and Horizontal (V&H) - Vertical and Horizontal coordinates result from a complex algorithm that projects the curvature of the earth onto a flat plane. These coordinates have been used in telephony since the late 1950's as a means to determine "airline" distance between two points via a simple formula. The projection algorithm uses latitude and longitude as well as various other factors in deriving V&H values. V&H's are used to identify locations and hence relative distances between network elements (e.g. switch locations), and between "rate centers" (e.g. the "center" of a rate exchange area). Such computations are necessary in cases where rates and costs for services are based on distance sensitive factors.
Very Early Smoke Detection Apparatus (VESDA) - A highly sensitive aspirating smoke detector installed in a data center is linked to the building management system which is monitored continually from a network operations centre, providing very early detection to help avoid fire, loss and business disruption. This is coupled with a gas based fire retardant that is environmentally friendly to put out fires instantly without damaging equipment.
Virtual Private Network (VPN) - Secure private communication path(s) through one or more non-private data networks that function as dedicated links between those points. To the users a VPN looks like a private network made up of dedicated links such as T1 or T3 lines. VPN connections allow data to safely and privately pass over public networks (such as the Internet).The data traveling between two points is encrypted for privacy.
Voice over Internet Protocol (VoIP) - A combination of technology and Internet protocols that allow the transmission of real-time voice communications across a data network.
Wavelength Division Multiplexing (WDM) - A method of transmitting several distinct communication channels through a single optical fiber via the use of a distinct separate infrared wavelength (optical frequency or "color") for each communication channel. Each such channel may be further subdivided into several logical channels via time division multiplexing or other methods**.**
Web Browser - Client software for connecting to and viewing documents on the WWW. A browser interprets HTML documents and displays them.
Web Browser/Server (WBS) - A Web Browser, a Web Server and their intended interaction. Web Browsers and Servers may communicate over the Internet and/or intranets.

Web Server - A Web site including hardware and software that includes the operating system, Web software, other software and data, or the software that manages Web functions at a Web site and makes web pages available to users.
Web Site - A computer on the Internet or an intranet running a Web Server that responds to HTTP and HTTPS request from Web Browsers.
Web-based - *See Web-based Media.*
Web-based Media - Distribution media by which electronic documents, reports, or files are provided or delivered to the government via a Hyper-Text Transmission Protocol (HTTP) server over the Internet.
Wide Area Network (WAN) - A communications network serving geographically separate areas. A WAN can be established by linking together two or more metropolitan area networks, which enables data terminals in one city to access data resources in another city or country.
Wire Center – The location of one or more local switching systems; a point at which customer loops converge.
Wire Center Serving Area – The area of an authorized telephone company's Local Exchange Service local calling area served by a single wire center.
Wireless - A categorization of switched and non-switched service types that generally use radio (e.g., mobile, cellular, or satellite radio) as their primary transmission medium. Generally excludes point-to-point terrestrial microwave.
Wireless Priority Service (WPS) - Wireless Priority Service (WP) allows authorized National Security and Emergency Preparedness personnel to gain priority access to wireless networks to initiate calls during an emergency when channels are congested.
Wireline - A categorization of switched and non-switched service types that generally use metallic cable, optical fiber cable, and point-to-point terrestrial microwave radio as their primary transmission media.
World Wide Web (WWW) - An Internet function for sharing of documents with text and graphic content that links documents locally and remotely.

J.13 List of Links

This section lists selected URLs referred to in this RFP.

J.13.1 Contracts/Federal Mandates/Executive Orders

FAR: https://www.acquisition.gov/?q=browsefar Clinger Cohen: https://www.fismacenter.com/Clinger%20Cohen.pdf

Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

Past Performance Information Retrieval System (PPIRS): http://www.ppirs.gov/

OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies: http://www.whitehouse.gov/omb/memoranda_2004

Electronic Product Environmental Assessment Tool (EPEAT):

https://www.epa.gov/greenerproducts/electronic-product-environmental-assessment-tool-epeat GETS Service:

- http://www.dhs.gov/government-emergency-telecommunications-service-gets

Wireless Priority Service (WPS):

- https://www.dhs.gov/wireless-priority-service-wps

Bureau of Labor Statistics (BLS) Department of Labor Employment and Training Administration's Occupational Information Network (O*NET):

http://www.onetonline.org/ BLS indices:

- Employment Cost Index (ECI): http://www.bls.gov/news.release/eci.toc.htm
- Producer Price Index (PPI): http://www.bls.gov/ppi/

J.13.2 Security

FIPS and NIST 800 Series: http://csrc.nist.gov/publications/index.html

FISMA: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

FedRAMP: http://www.FedRAMP.gov

- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and contractors," August 27, 2004; available at: http://www.idmanagement.gov/.

J.13.3 GSA

Network Services Program: http://www.gsa.gov/portal/category/22151

Core Based Statistical Areas (CBSAs):

- http://www.census.gov/geo/reference/gtc/gtc_cbsa.html
- http://www.whitehouse.gov/sites/default/files/omb/bulletins/2013/b-13-01.pdf

J.14 Form DD254

GSA FAS ITS EIS Top Secret Form DD254 0

J.15 Calculation of Economically Adjusted Prices (EAP)

EPA V.2.1.xlsx

J.16 Instructions for Gaining Access to AcquServe

J.16.1 AcquServe Access Guide for EIS (FEB 2015)

AcquServe Access Guide for EIS Feb 201

J.16.2 Agreement to Protect Sensitive Information

Agreement to Protect Sensitive Infc

J.16.3 EIS Offeror Application

EIS Offeror Application.doc

J.16.4 List of Designated Users

List of Designated Users.doc

J.17 AcquServe User Instructions

Refer to AcquServe, https://acquserve.eis.noblis.org for current version of User Guide.

J.18 DARS and DFARS Clauses

EIS DARS and DFARS Clauses.docx

J.19 Submission Matrix

Submission Matrix J.19 Amendment 12.x

J.20 Small Business Subcontracting Plan Outline (Model)

Section J Subcontracting Plan A

HARRIS CORPORATION
Government Communications Systems

RFP No. QTA0015THA3003

(b) (2), (b) (4)

Volume 5—Subcontracting

Final Proposal Revisions #2

Enterprise Infrastructure Solutions (EIS)

For:
General Services Administration
Office of Integrated Technology Services
(b) (2), (b) (4)

Attention:
FAS EIS Contracting Officer

Telephone (703) 306-6426
Timothy.Horan@gsa.gov

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

1.0 SUBCONTRACTING PLAN AND SUBCONTRACTING PARTICIPATION

INDIVIDUAL SUBCONTRACTING PLAN

IDENTIFICATION DATA:

Identification Data	
Company Name:	Harris Corporation Government Communications Systems
Mailing Address:	P.O. Box 37, Melbourne, FL 32902
Physical Address:	2400 Palm Bay Road SE, Palm Bay, FL 32905
Cage Code:	91417
DUNS	021715206
Solicitation or Contract Number:	(b) (2), (b) (4)
Item / Service:	GSA ENTERPRISE INFRASTRUCTURE SOLUTIONS (EIS)
Individual Contract Period:	(b) (2), (b) (4)
Date Prepared:	(b) (2), (b)
Plan Period:	(b) (2), (b) (4)

This Individual Subcontracting Plan contains all the elements required by FAR 52.219-9 "Small Business Subcontracting Plan" and shall apply throughout the life of the contract. Harris will comply with all elements of FAR 52.219-9 and GSAM Provisions 552.219-72 and 552.219-73. This Individual Subcontracting Plan, together with Attachment to cover Individual Subcontracting Goals, is prepared to satisfy the applicable requirements of Public Laws 95-507, as amended, 100-656, 103-355, 105-135 and 106-50.

TABLE OF CONTENTS

1.0 INTRODUCTION

Harris Corporation is a large international communications and information technology company whose businesses serve the U.S. federal government and, commercial markets worldwide. Harris Corporation is headquartered in Melbourne, Florida, has approximately $6 billion in annual revenue and more than 17,000 employees worldwide — including 7,700 engineers and scientists. **Harris Government Communications Systems** (hereinafter referred to as Harris GCS) is an operating segment within Harris Corporation. **Harris GCS** serves a diversified customer base whose major customers consist of the Department of Defense (DoD), Federal Aviation Administration (FAA), National Oceanic and Atmospheric Administration (NOAA), National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), General Services Administration, NASA, national intelligence programs, and various other U.S. Government agencies, as well as commercial clients and other industries and agencies. **Harris GCS** specializes in airborne, spaceborne, ground-based and maritime communications and develops information processing and communications systems for the U.S. Government as well as for state and local governments and industry.

1.1 Supplier Diversity Commitment

Harris GCS is *committed* to providing Small Business, Small Disadvantaged Business, Women-Owned Small Business, HUBZone Small Business, Veteran-Owned Small Business, and Service-Disabled Veteran-Owned Small Business Concerns maximum practical opportunity to participate as suppliers for Harris GCS purchased materials and services. We actively seek Small Business Concerns who share our high standards of quality, service, timeliness and low cost. We encourage participation from qualified, innovative, and competitive Small Business, Small Disadvantaged Business, Women-Owned Small Business, HUBZone Small Business, Veteran- Owned Small Business, and Service-Disabled Veteran-Owned Small Business Concerns.

Harris GCS has a division-wide Small Business program policy statement issued by current senior management, disseminated throughout the company. The Small Business program policy statement is reviewed annually and changed accordingly.

1.2 Small Business Program Implementation

Harris GCS has a division-wide Supplier Diversity program, encompassing DoD, to solicit and use Small Businesses in the execution of contracts, and a Small Business Office with a support team dedicated to focusing its resources on increasing subcontracting opportunities for Small Business concerns with a total division approach. Awareness is promoted through monthly Small Business Council meetings, a forum where Small Business procurement results are presented and areas for improvement are discussed with Supply Chain senior management.

Harris GCS received a "Highly Successful" rating of its GFY 2014 Small Business Program as a result of a review conducted May 2015 by Defense Contract Management Agency per *June 19, 2015 letter from Margarette Trimble-Williams, Assistant Director, DCMA Small Business Center.*

Harris GCS received a Champions of Veterans Enterprise Award in the category of Corporate Achievement from the U.S. Department of Veterans Affairs Center for Veterans Enterprise for exceeding the criteria of $1 million dollars or more in awards to Service-Disabled Veteran-Owned Small Businesses (SDVOSB) and exceeding the 3 percent SDVOSB subcontracting goal.

Figure 1.0. Champions of Veterans Enterprise Award

Harris GCS is the proud recipient of the Dwight D. Eisenhower Award for Excellence, Research and Development Category. This Award is bestowed by the U.S. Small Business Administration to prime contractors that have excelled in their utilization of small businesses as subcontractors and suppliers.

(b) (2), (b) (4) [redacted]

Harris GCS promotes Small Businesses at all levels of activity throughout the division, Harris company-wide and within the Small Business Community. The many avenues include: providing opportunities for Small Businesses to showcase their technologies during supplier events; hosting Small Business opportunity meetings with Harris engineering/Supply Chain personnel; seeking Small Businesses utilizing the Harris GCS internal prospective supplier database, the SBA's Dynamic Small Business Search and HUBZone locator tools, VetBiz.org and state, local and federal resources.

(b) (2), (b) (4)

2.0 POLICY

Harris GCS is committed to providing Small Business, Small Disadvantaged Business, Women-Owned Small Business, HUBZone Small Business, Veteran-Owned Small Business, and Service-Disabled Veteran-Owned Small Business Concerns maximum opportunity to participate as suppliers for Harris GCS purchased materials and services. Harris actively seeks Small Business Concerns who share our high standards of quality, service, timeliness and low cost. Harris encourages participation from qualified, innovative, and competitive Small, Small Disadvantaged Business, Women-Owned, HUBZone, Veteran-Owned and Service-Disabled Veteran-Owned

Small Business concerns. The following policy statements demonstrate Harris GCS support of the Small Business Program:

(b) (2), (b) (4)

- (b) (2), (b) (4)
- (b) (2), (b) (4)

2.2 Implementation of Company Policy and Procedures

- **Small Business Utilization Requirements.** Small Business utilization is a responsibility for each procurement personnel responsible for placing orders and Supply Chain Management. Proposal and procurement personnel utilize the Harris GCS Prospective Supplier Database to assist in research of Small Business Concerns for partnering or subcontracting opportunities. Solicitation/Supplier selection is

documented on all awards of $150K through the use of Harris form "Small Business Checklist". For awards over $700,000 to other than Small Business Concerns, a subcontracting plan is required to ensure flowdown subcontracting opportunities exist for Small Business Concerns. The Small Business Checklist is reviewed by the buyer's manager and then reviewed by the Small Business Office to ensure Small Business Concerns are utilized at every possible opportunity.

- **Small Business Prospective Supplier Database and Other Sourcing Tools.** The SBLO is responsible for maintenance of the Prospective Supplier Database, which contains information on existing and potential Small Business suppliers to Harris GCS. Small Businesses are encouraged to submit their Profile form to be included in this system by accessing an external web page http://govcomm.harris.com/suppliers/smallbusiness/. All Harris GCS personnel are able to search this database by company name, state, category (commodity), Small Business code, supplier type or keyword to locate potential sources for their procurement opportunities. The SBLO is available and is frequently called upon to assist procurement personnel in identifying Small Business Concerns with products and services that meet the quality and reliability requirements of the program by utilizing the Harris GCS Prospective Supplier Database, Dynamic Small Business Search (DSBS), VetBiz.gov (U.S. Dept. of Veterans Affairs database), FAA's Source.net, and other federal, state and local resources, and the internet. Harris GCS uses the System for Award Management (SAM) to assist the validation of supplier size and subcategory status.
- **Small Business Council, Role and Responsibilities.** Harris GCS management requires program and procurement personnel to be directly involved in the achievement of the Small Business Plan and goals. The SBLO chairs monthly meetings of the Small Business Council who have responsibility for oversight of the Small Business Program. The Small Business Council provides a forum where current and year-to-date data is presented, areas for improvement are discussed, improvement action plans are undertaken where necessary, and awards are presented. The Small Business Council is comprised of Supply Chain senior management. Individual contributors, including Senior Managers, are responsible for

ensuring Harris' Small Business policies are appropriately implemented in their programs. Quantifiable Small Business objectives are incorporated into performance evaluations for senior management, individual materiel management and procurement personnel identified as key results expected.

3.0 DEFINITIONS

As used in the context of this plan, the following terms are defined:

- ***"Small Business"*** means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on government contracts, and qualified as a Small Business under the criteria and size standards in 13 CFR Part 121. Such a concern is "not dominant in its field of operation" when it does not exercise a controlling or major influence on a national basis in a kind of business activity in which a number of business concerns are primarily engaged. In determining whether dominance exists, consideration must be given to all appropriate factors, including volume of business, number of employees, financial resources, competitive status or position, ownership or control of materials, processes, patents, license agreements, facilities, sales territory, and nature of business activity. (See 15 U.S.C. 632.)
- ***"Small Disadvantaged Business (SDB)"*** means a Small Business concern that is at least 51 percent owned by one or more individuals who are socially and economically disadvantaged, or a publicly owned business having at least 51 percent of its stock owned by one or more socially and economically disadvantaged individuals and has its management and daily business controlled by one or more such individuals. This term also means a Small Business concern that is at least 51 percent unconditionally owned by an economically disadvantaged Indian-Owned tribe or Native Hawaiian Organization, or a publicly owned business having at least 51 percent of its stock unconditionally owned by one or more of these entities, which has its management and daily business controlled by members of an economically disadvantaged Indian-Owned tribe or Native Hawaiian Organization, and that meets the requirements of 13 CFR 124.

- ***"Women-Owned Small Business (WOSB)"*** means a firm which meets the above criteria as a Small Business and which is at least 51 percent owned by one or more women; or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women, and whose management and daily business operations are controlled by one or more women.
- ***"HUBZone Small Business (HZSB)"*** means a small business concern that appears on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration (13 CFR 126.103). HUBZone means a historically underutilized business zone that is an area located within one or more qualified census tracts, qualified non-metropolitan counties, lands within the external boundaries of an Indian reservation, qualified base closure areas, or redesignated areas, as defined in 13 CFR 126.103.
- ***"Veteran-Owned Small Business (VOSB)"*** means a Small Business concern not less than 51 percent of which is owned by one or more veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and the management and daily business operations of which are controlled by one or more veterans.
- ***"Service-Disabled Veteran-Owned Small Business (SDVOSB)"*** means a "Small Business concern owned and controlled by service-disabled-veterans" (as defined in section 101 (16) of title 38, United States Code**)**; not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and the management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a veteran with permanent and severe disability, the spouse or permanent caregiver of such a veteran."
- **"*Historically Black Colleges and Universities (HBCU's)"*** means institutions determined by the Secretary of Education to meet the requirements of 34 CFR Section 608.2.

- ***"Minority Institutions (MI's)"*** means institutions meeting the requirements prescribed by the Secretary of Education at 34 CFR 607.2. The term also includes any nonprofit research institution that was an integral part of a historically black college or university before November 14, 1986.
- ***"Indian"***---any person who is a member of any Indian tribe, band, group, pueblo, or community that is recognized by the Federal Government as eligible for services from the Bureau of Indian Affairs (BIA) in accordance with 25 U.S.C. 1452(c) and any "Native" as defined in the Alaska Native Claims Settlement Act (43 U.S.C. 1601) or Native Hawaiian organization as defined by 15 U.S.C. 637(a)(15) and 13 CFR 124.3.
- ***"Indian-owned/Economic Enterprise"***--any Indian-owned (as determined by the Secretary of the Interior) or Native-owned commercial, industrial, or business activity established or organized for the purpose of profit, provided that Indian ownership constitutes not less than 51 percent of the organization.
- ***"Indian tribe"*** means any Indian tribe, band, group, pueblo, or community, including native villages and native groups (including corporations organized by Kenai, Juneau, Sitka, and Kodiak) as defined in the Alaska Native Claims Settlement Act (43 U.S.C.A. 1601 et seq.), that is recognized by the Federal Government as eligible for services from the Bureau of Indian Affairs in accordance with 25 U.S.C. 1452(c). This definition also includes Indian-owned economic enterprises that meet the requirements of 25 U.S.C. 1452(e).
- ***"Alaska Native Corporation (ANC)"*** means any Regional Corporation, Village Corporation, Urban Corporation, or Group Corporation organized under the laws of the State of Alaska in accordance with the Alaska Native Claims Settlement Act, as amended (43 U.S.C. 1601, *et seq.*) and which is considered a minority and economically disadvantaged concern under the criteria at 43 U.S.C. 1626(e)(1). This definition also includes ANC direct and indirect subsidiary corporations, joint ventures, and partnerships that meet the requirements of 43 U.S.C. 1626(e)(2).

4.0 GOALS - FAR 52.219-9(d)(1-2)

Small Business goals will be established for each solicitation/contract and will be indicated on Attachment A of the Individual Subcontracting Plan. The goals will include

percentages and dollars for the following Small Business concerns: Small, Small Disadvantaged, Women-Owned, HUBZone, Veteran-Owned and Service-Disabled Veteran Owned. The values represent estimated procurement award dollars (i.e., purchases of products, supplies and services planned to be subcontracted); the percentage of planned subcontracting to total planned subcontracting; and, the percentage of planned subcontracting to total contract value, if customer required. The Individual Subcontracting Plan shall include a separate goal for the basic contract and if applicable, each option.

5.0 PRINCIPAL SUPPLIES & SERVICES – FAR 52.219(d)(3)

Principal Supplies and Services that Harris anticipates to be acquired and the identification of the type of business concern planned will be established for each solicitation/contract and will be indicated on Attachment A of the Individual Subcontracting Plan.

6.0 METHODS USED TO DEVELOP SUBCONTRACTING GOALS - FAR 52.219-9(d)(4)

Harris determines the total expected outsourcing based on the contract scope as the primary driver, and on technical needs and current in-house capabilities, some of which are estimates at the time of proposal submittal based on defined scope and Small Business candidate capabilities. Small Business candidates continue to be identified and qualified through the execution of the contract in order to maximize the level of outsourced activities to maintain or exceed the stated Small Goals. We also assess other possible sources of supplier involvement to help implement the scope of work in order to meet and/or exceed goal requirements. Hardware, supplies, and services to be acquired are determined through supplier profiles, demonstrated capabilities, and existing Small Business supplier relationships. This activity continues through the execution of the contract as the details of program needs evolve.

Goals are established to comply with the requirements of the Federal Acquisition Regulations (FAR) 19.7 “The Small Business Subcontracting Program; FAR 52.219-8 “Utilization of Small Business Concerns”; and FAR 52.219-9 “Small Business Subcontracting Plan”; Public Law; and, the Request for Proposal.

7.0 METHODS USED TO IDENTIFY POTENTIAL SOURCES - FAR 52.219-9(d)(5)

To identify potential sources for solicitation purposes, we provide opportunities for Small Businesses to showcase their technologies during supplier events and at hosted Small Business opportunity meetings with engineering/supply chain personnel. In addition, to search for potential suppliers in all Small Business subcategories, we use our database of current Small Businesses; our internal prospective supplier database (a web-based portal); the Dynamic Small Business Search tool; the U.S. Department of Veterans Affairs Center for Veteran's Enterprise web portal for Veterans in business (www.VetBiz.gov); and additional state, local, and federal Supplier Diversity databases. Also, we proactively seek SB suppliers through various resources which include, but are not limited to:

Small Business Development Centers (SBA)

Procurement Technical Assistance Centers (DoD)

National/Florida Minority Supplier Development Council

Advocacy and Trade Association Directories (Federal, state, and local level)

Supplier Diversity Conferences and Business Trade Fairs

Women's Business Center at Florida Institute of Technology

DoD Mentor-Protégé Conference

7.1 Activities to Identify & Develop Potential Sources

Harris GCS participates in activities to identify, develop and assist Small Business Concerns. Some of these activities include:

- Provide information to Small Business Concerns regarding procurement procedures and bidding methods, as well as provide appropriate assistance necessary to ensure that these firms have the maximum practicable opportunity to compete for available subcontracts and purchase orders.
- (b) (2), (b) (4) [redacted]

- (b) (2), (b) (4) [redacted]
- Evaluate Subcontractors' Subcontracting Plans for Small Business Concerns when required by the Federal Acquisition Regulations.
- (b) (2), (b) (4) [redacted]
- Conduct "Supplier Opportunity Meetings" to provide an additional forum for Small Businesses to present their products or services to Harris GCS' buying community.
- **Harris GCS** generates press releases regarding our Small Business events and activities in support of assistance to our Small Business Concerns. Local media as well as national publications typically pick up these press releases.
- Harris participates in government/industry conferences and trade fairs, committees, organizations and councils dedicated to assisting Small Businesses. In addition, many of these also assist industry in the efficient development and performance of their Small Business Programs, such as
  - National 8(a) Association Conference
  - Florida 8(a) Alliance Small Business Conference
  - National MED (Minority Enterprise Development) Week
  - Florida Minority Supplier Development Council (FMSDC) Space Coast Chapter meetings
  - FMSDC Supplier Trade Fair
  - National Minority Supplier Development Council Supplier Expo
  - National Reservation Economic Summit (RES) / American Indian Business Trade Fair

- National Veterans Small Business Conference
- SBDC Brevard County (FL) Veteran-Owned Small Business Conference
- NASA / Kennedy Space Center Expo
- OSDBU Council Annual Government Procurement Conference
- National Small Business Contracting Summit – Southeast (U.S. Women's Chamber of Commerce)
- MidWest Small Business Government Contracting Symposium (Rock Island Contracting Center)
- PTAC sponsored (e.g. University of Central Florida Government Opportunities Event)
- Congressman Bill Posey Federal Contracting Conference
- Brevard County (FL) Small Business Assistance Council (BSBAC) meetings
- TRI-Association Small Business Advisory Panel (TRIAD) meetings
- NDIA National Small Business Conference
- Missile Defense Agency Small Business Programs Conference
- Defense Procurement Summit (e.g. Orlando)
- DoD Mentor-Protégé Conference
- Manufacturing Innovation Conferences
- Florida Manufacturing Extension Partnership Lean Training events
- Dept of Interior Small Business Outreach Workshops
- Alliance of Supplier Diversity Professionals Meetings & Training Conferences
- TechXPO, Florida Institute of Technology

- (b) (2), (b) (4) [redacted]
- Subscribing to several supplier information directories/publications and established contacts with national and regional Minority Purchasing Development Councils. Additionally, Harris GCS interfaces with other large prime contractors for the purpose of source/information gathering and data exchange.

- Continue Harris GCS Supply Chain Management emphasis on special efforts to seek Small Businesses qualified to furnish subcontracted materials and services. This effort includes assistance in every reasonable manner to develop new potential sources.

8.0 INDIRECT COSTS – FAR 52.219-9 (d) (6)

INDIRECT AND OVERHEAD COSTS have not been included in the goals described in Attachment A of the Individual Subcontracting Plan.

9.0 ADMINISTRATION OF PLAN - FAR 52.219-9(d)(7)

The Harris GCS Small Business Liaison Officer (SBLO) promotes the Small Business Program objectives at all levels of activity within Harris GCS and the Small Business Community. It is the responsibility of the Harris GCS SBLO, appointed December 2004 by the Harris GCS President, to maintain a program compliant with Public Laws 95-507 and 100-656, 10 USC Section 2323, DFARS 252.219-7004, The Small Business Act, The Small Business Investment Act, Small Business Reauthorization Act of 1997, Utilization of Small Business Concerns, Subcontracting Plans for Small Business Concerns, and to assure that Small Business Concerns, and Indian-Owned Organizations will have an equitable opportunity to compete for orders within their capabilities.

This plan will be administered by:

Contact Information	
(b) (2), (b) (4) [redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

9.1 Responsibilities

- Implementation of the Small Business Jobs Act of 2010, amended by the Small Business Act, effective August 27, 2013 (CFR Parts 121, 124, 125, 126 and 127) dealing with Small Business size and status integrity.
- Implementation of the Small Business Jobs Act of 2010, amended by the Small Business Act, effective August 15, 2013 (CFR Parts 121 and 125) dealing with Small Business Subcontracting.

- In accordance with Public Law 106-50, "The Veterans Entrepreneurship and Small Business Development Act of 1999", Harris GCS' SBLO is the designated veteran coordinator.
- Division advisory on matters relating to the use of Small Business Concerns and represent the organization in matters relating to Public Law 95-507 and other related Federal laws and regulations.
- Issue and promulgate policy statements and internal operating instructions to implement the requirements of Public Law 95- 507 and other applicable Government regulations.
- Develop Small Business Subcontracting Plans for Small Business Concerns. Manage and administer all aspects of the Small Business Subcontracting Plan goals and program initiatives.
- **Promote Small Business Concerns.** Actively promotes and provides Small Business, Small Disadvantaged, Women Owned, HUBZone, Veteran-Owned, Service-Disabled Veteran-Owned Small Business concerns, and Native American Indian-owned economic enterprises the opportunity to showcase their products and services to Harris GCS supply chain and engineering personnel.
- **Sponsor/Host Small Business Opportunity Meetings** including "industry day" small business fairs, sponsor seminars for the Small Business community; conduct business-to-business matchmaking and participate in Small Business supplier events such as Reservation Economic Summit (RES), National Veterans Small Business Conference, MED (Minority Enterprise Development) Week, FAA National Small Business Procurement Opportunities Training Conference, Florida Minority Supplier Development Council Conference, Annual NASA Kennedy Space Center Expo, OSDBU (Offices of Small and Disadvantaged Business Utilization) Procurement Conference, DoD Mentor-Protégé Conference, and other national, regional and Florida supplier events identified throughout the year.
- **Undertake special efforts to increase the dollar value of procurements** directed to Small Business concerns by reviewing monthly reports to determine where dollars are being spent, researching options to divert procurements from large

to small or small "subcategories", and encourage procurement to utilize identified sources in future procurements.

- **Small Business Search/Outsource Assistance.** Assist Supply Chain, Engineering, Business Development, Program/Capture Management and Proposal personnel in identifying Small Business concerns that offer products and services that meet the quality and reliability requirements of the program by utilizing the Harris GCS Prospective Supplier Database, the U.S. Small Business Administration's (SBA) Dynamic Small Business Search, the SBA HUBZone Locator, DoD Procurement Technical Assistance Centers, SBA Small Business Development Centers, U.S. Department of Veterans Affairs Center for Veterans Enterprise web portal, state and local resources, and the internet. Provide and maintain on-line access to Dynamic Small Business Search, which provides an additional database of potential Small Business Concerns across all product and services.
- **Maintain Ongoing Outreach Program.** Enhance Small Business participation in Harris GCS programs by working with the Supplier Focus teams to review and identify capabilities of potential Small Business suppliers, visit successful Small Business suppliers to gather data that can enhance other Small Businesses and assist buyers with outreach, facilitate resolution of supplier problems to ensure success of a supplier whenever feasible, coordinate and/or conduct on-site "Supplier Opportunity" meetings with SBLO and/or procurement, proposal and engineering community, conduct monthly Small Business Council Meetings to apprise Supply Chain management of the division's performance against goals, identify opportunities for improvement, conduct annual training to the buying community of the Small Business Program, and host/sponsor a minimum of two Supplier events annually.
- **Expanding Small Business Supplier Base.** Participate in all activities associated with the expansion of the Small Business supplier base; administer Prospective Supplier Database for use by Harris GCS personnel seeking new Small Business Concerns, ensure Small Business Concern inclusion on Harris GCS Supplier Focus teams (commodity matrices), participate in activities of regional and national minority

councils and organizations, direct new suppliers to the appropriate Harris GCS contacts, participate in trade fairs and government/industry conferences.

- **Industry Representation.** Participate as an active member in the Tri-Association Small Business Advisory Panel (TRIAD), a forum for information exchange between large and small/small disadvantaged businesses; the Florida Minority Supplier Development Council; the Brevard Small Business Assistance Council; and, the Alliance for Supplier Diversity Professionals, a forum to increase professional development, and enhance customer relations to effect a positive growth of individual organizations' supplier diversity programs.
- **Small Business Reports and Surveys.** Submit small business subcontracting achievement data on the Subcontracting Report for Individual Contracts, and/or Summary Subcontract Report, using the Electronic Subcontracting Reporting System or eSRS at www.esrs.gov. Submit Comprehensive Subcontracting Plan Initiatives/Industry Category performance reports; Mentor-Protégé Program semi-annual and annual reports. Cooperate in studies or surveys required by contracting agencies and the U.S. Small Business Administration (SBA); assist SBA Commercial Market Representative and Federal Government agencies involved in periodic reviews and/or opportunity referrals.
- **Small Business Goal Development & Performance to Goal Oversight.** Participate in the establishment of goals and objectives and keep Small Business Council apprised of progress towards goal/objective accomplishment. Oversee data collection, and distribute and display reports that reflect progress toward the achievement of Small Business goals.
- **Mentor-Protégé Program.** Evaluate supplier candidates for Mentor-Protégé relationships. Conduct needs assessments and make recommendations as to the feasibility of an agreement based on supplier capabilities match with Harris technologies and supplier capacity to undertake a formal agreement. Guide and/or develop new agreements. Orchestrate informal mentoring and/or collaborative assistance opportunities between Harris and Small Businesses.

- **Small Business Utilization Training.** Develop and/or sponsor programs that provide training to Harris GCS personnel on issues relative to the Small Business Program, utilization of Small Business Concerns and related federal laws and regulations, subcontracting plans, and divisional performance. This training is provided annually and when required under special circumstances (e.g., for new hires).
- **Small Business Council.** Harris GCS management requires program and procurement personnel to be directly involved in the achievement of the Small Business Plan and goals. The SBLO chairs monthly meetings of the Small Business Council. The Small Business Council provides a forum where current and year-to-date data is presented, displayed, areas for improvement are discussed, improvement action plans are undertaken where necessary, and awards are presented. The Small Business Council is comprised of Supply Chain senior management. Individual contributors, including Senior Managers, are responsible for ensuring Harris' Small Business policies are appropriately implemented in their programs. Quantifiable Small Business objectives are incorporated into performance evaluations for Senior Management, individual Materiel Management and Procurement personnel identified as key results expected.
- (b) (2), (b) (4) [redacted]
- **Small Business Assistance.** Provide assistance to Small Business Concerns on becoming a supplier to Harris GCS including an overview of Harris GCS processes and procedures, organizational structure, and issues relating to performance as a supplier to Harris GCS. The SBLO will facilitate resolution of problems to ensure success of a supplier whenever feasible. The SBLO also provides guidance to Small

Business Concerns regarding the Federal Government's Small Business program initiatives and resources available through the Small Business Administration, Procurement Technical Assistance Center, SCORE and other government agencies.

10.0 EFFORTS TO ENSURE EQUITABLE OPPORTUNITY – FAR 52.219-9(d)(8)

Harris GCS makes every effort to ensure that Small, Small Disadvantaged, Women-Owned Small, HUBZone Small, Veteran-Owned and Service-Disabled Veteran-Owned Small Business concerns have an equitable opportunity to compete for subcontracts. These efforts include, but are not limited to, the following activities:

A. Outreach efforts to obtain sources, particularly new sources possessing innovative technologies/techniques:
   - Contacting minority and small business trade associations
   - Contacting business development organizations, including Federal Agency Office of Small Business Programs for newly identified firms
   - Seeking Small Business sources of supply using the SBA Dynamic Small Business Search tool (Note: System for Award Management www.SAM.gov is utilized to verify business size / Small Business status.)
   - Attending industry conferences looking for emerging technologies from Small Business Concerns
   - Attending Small, Minority, and Women-Owned Small Business procurement conferences and trade fairs
   - Hosting Small Businesses at key program events
   - Requesting referrals from Small Businesses for future consideration

B. Internal efforts to guide and encourage purchasing personnel:
   - Presenting workshops, seminars, and training programs
   - Establishing, maintaining, and using source lists, guides, and other data for soliciting subcontracts from Small Business Concerns
   - Monitoring activities to evaluate compliance with the subcontracting plan

C. Additional efforts:
   - Leverage the experience and support of our other divisions and company businesses to continuously improve our SB Program

- Continue our mentoring efforts to provide continuing new business opportunities and technical assistance
- Proposal personnel ensure that adequate and timely consideration is given to Small Businesses in all "make-or-buy" decisions for those items that have been identified for procurement from external sources

10.1 HUBZONE SMALL BUSINESS CONCERNS

In accordance with the HUBZone Act of 1997, Harris GCS gives maximum consideration to qualified, prospective and active HUBZone suppliers for procurement requirements. Harris GCS utilizes the *Dynamic Small Business Search tool* and HUBZone locator to identify HUBZone Small Business Concerns for potential subcontracting opportunities for U.S. government agency program requirements. The Small Business Office will continue to encourage additional participation of HUBZone Small Businesses.

10.2 NATIVE AMERICAN INDIAN OWNED ECONOMIC ENTERPRISES

Native American Indian- Owned economic enterprises are given maximum consideration as potential Small Business sources. Harris GCS procurement procedures address the utilization of Native American Indian owned organizations. Small Business codes are identified in Harris GCS' database in order to facilitate solicitation, award, monitoring and reporting of performance. Harris GCS emphasizes the utilization of Native American Indian Owned economic enterprises and continues to review opportunities that may utilize the Indian Incentive Program (FAR Subpart 26.1).

Harris GCS has identified the Bureau of Indian Affairs for dedicated business opportunities and actively participates in and exhibits at the Annual Reservation Economic Summit (RES) and American Indian Business Trade Fair.

10.3 VETERAN-OWNED AND SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS CONCERNS

In accordance with Public Law 105-50, "The Veteran's Entrepreneurship & Small Business Development Act of 1999", Harris GCS gives maximum consideration to qualified, prospective and active Veteran-Owned Small Businesses (VOSB), and Service-Disabled Veteran-Owned Small Businesses (SDVOSBs) so they may participate as

subcontractors for procurements. Harris GCS reviews the lists of VOSBs and SDVOSBs registered in federal databases for potential subcontracting opportunities for government agency program requirements and will solicit VOSBs and SDVOSBs, when feasible.

Harris annually participates in the Department of Veterans Affairs' Annual National Veterans Small Business Conference. Harris also supports other Veteran Conferences, and conducts business-to-business supplier opportunity meetings in conjunction with Supply Chain and Engineering personnel.

10.4 Education and Training

Harris GCS is committed to the continuation of internal education and training relative to Small Business Program policies and regulations. Training is conducted by the Small Business Office to ensure that all program procurement, material management, subcontracts and proposal pricing personnel are adequately educated on issues relating to Small Business concerns, related laws/regulations, and the resources available to maximize Small Business utilization. This training is provided annually and when required under special circumstances (e.g., for new hires).

10.5 METHODS OF PUBLICIZING SUBCONTRACT OPPORTUNITIES

Harris GCS publicizes prospective subcontract opportunities by participating in Federal procurement conferences, trade fairs, industry conferences, business-to-business matchmaking and related functions and presentations to local organizations such as Harris hosted chapter meetings of the Florida Minority Supplier Development Council, Eastern Florida State College Veterans Conference (SBDC/PTAC), Economic Development Commission of Florida's Space Coast, regional minority purchasing councils and Small Business development centers. Harris GCS' Small Business web site includes a Prospective Supplier Profile Form, which suppliers fill out and submit to the Harris GCS Small Business Office.

Strategic Sourcing Teams

Harris GCS utilizes Supplier Focus Teams for some products and services which may be outsourced. Each Focus Team contains suppliers who are pre-approved by the Supplier Management Committee for doing business with Harris GCS. Products and services vary depending upon program content and requirements.

Open Postings/Electronic Bidding

Harris does not engage in open postings or electronic bidding due to the nature of our work and the customer base we serve (intelligence community, DoD, other federal agencies). Harris GCS is the corporation hub for research and development.

11.0 SUBCONTRACT FLOWDOWN – FAR 52.219-9(d)(9)

Harris GCS agrees to include in this contract FAR clause number 52.219-8, titled "Utilization of Small Business Concerns" in all procurement actions that offer further supplier opportunities. Harris will further require all suppliers (except small business concerns) who receive orders in excess of $700,000 ($1,500,000 for construction of any public facility) to adopt a subcontracting plan that complies with the requirements of the clause at FAR 52.219.9 entitled, "Small Business Subcontracting Plan". Such plans will be reviewed by comparing them with the provisions of P.L. 95-507 and assuring that all minimum requirements of acceptable subcontracting plan have been satisfied. The acceptability of percentage goals shall be determined on a case-by-case basis depending on the supplies/services involved, the availability of potential SB, SDB, WOSB, HZSB, VOSB and SDVOSB subcontractors, and prior experience. Once approved and implemented, subcontracting plans will be monitored through the submission of periodic reports.

Harris GCS utilizes the following methods to ensure flow-down of required Small Business provisions to sub-tier subcontractors and suppliers:

- The flow-down of appropriate clauses, as required by Public Law 95-507 as well as other related Federal laws and regulations, is accomplished by incorporating these clauses into subcontracts by Harris' General Provisions. Harris GCS includes the clause at 52.219-8, Utilization of Small Business Concerns, in all subcontracts that offer further subcontracting opportunities, and requires all subcontractors (except Small Business Concerns) that receive subcontracts in excess of $700,000 ($1,500,000 for construction) to adopt a plan that complies with the requirements of the clause at 52.219-9, Small Business Subcontracting Plan.

12.0 REPORTING & COOPERATION – FAR 52.219-9 (d) (10)

Harris agrees to: (1) cooperate in any studies or surveys as may be required; (2) submit periodic reports which show compliance with the subcontracting plan; (3) submit Individual Subcontract Reports (ISR) and/or the Summary Subcontract Report (SSR) using the Electronic Subcontracting Reporting System (eSRS) at http://www.esrs.gov in accordance with requirements of this web-based reporting portal; (4) ensure our subcontractors with subcontracting plans agree to submit the ISR and/or the SSR using eSRS; (5) provide the prime contract number, Harris's DUNS number, and the e-mail address of the Harris official responsible for acknowledging or rejecting the reports, to all first-tier subcontractors with subcontracting plans so they can enter this information into the eSRS when submitting their reports; and (6) require our subcontractors with a subcontracting plan provide the prime contract number, its own DUNS number, and e-mail address of the subcontractor official responsible for acknowledging or rejecting the reports, to its subcontractors with subcontracting plans. After November 30, 2017, Harris will include subcontracting data for each order when reporting subcontracting achievements for indefinite-delivery, indefinite-quantity contracts intended for use by multiple agencies.

12.1 Subcontractor Report Requirements

Harris GCS requires subcontractors to submit Individual Subcontracting Plans when required, either to the cognizant government agency offices or to Harris GCS. Such Plans will include assurances that the subcontractor will: 1) cooperate in any studies or surveys as may be required; 2) submit periodic reports so that the Government can determine the extent of compliance by the subcontractor with the subcontracting plan; 3) submit the Individual Subcontract Report (ISR) using the Electronic Subcontracting Reporting System (eSRS) at http://www.esrs.gov . The reports shall provide information on subcontract awards to Small Business Concerns, Veteran-Owned Small Business Concerns, Service-Disabled Veteran-Owned Small Business Concerns, HUBZone Small Business Concerns, Small Disadvantaged Business Concerns, Women-Owned Small Business Concerns. Reporting shall be in accordance with agency regulations. Harris will ensure that its subcontractors with subcontracting plans agree to submit the ISR

using eSRS. Harris will provide its prime contract number, its DUNS number, and the e-mail address of the Government or Contractor official responsible for acknowledging or rejecting the reports, to all first- tier subcontractors with subcontracting plans so they can enter this information into the eSRS when submitting their reports; and require that each subcontractor with a subcontracting plan provide the prime contract number, its own DUNS number, and the e-mail address of the Government or Contractor official responsible for acknowledging or rejecting the reports, to its subcontractors with subcontracting plans. Harris employs a process whereby Harris buyers are notified that their subcontractors' ISRs are required and the due date; received ISRs are reviewed for performance to goal; ISRs are approved or rejected; received ISRs are recorded in a log.

12.2 Reporting Tool

Harris GCS has an automated statistical reporting system to assure accurate, timely reporting of Small Business data and information. The Small Business Report tool compiles procurement metrics according to supplier Small Business code and Harris GCS order type.

13.0 RECORDS MAINTAINED – FAR 52.219-9(d)(11)

Harris GCS agrees that it will maintain records to demonstrate that procedures have been adopted to comply with the requirements and goals with this Small Business Subcontracting Plan. These records include:

A. Source lists, guides and other data that identify Small Businesses, and Indian-Owned/Native American Organizations (i.e., Harris GCS Prospective Supplier Database, Supplier Focus Team matrices, SBA Dynamic Small Business Search, System for Award Management, various directories and Listings, etc.).

B. Records of organizations contacted to locate Small, Small Disadvantaged, Women, HUBZone, Veteran and Service-Disabled Veteran-Owned Small Business concerns, and Native American Indian-Owned economic enterprises.

C. Records on each subcontract solicitation resulting in an award of more than $150,000, indicating whether Small Business Concerns were solicited and, if not, why not; (2) whether Small Disadvantaged Business concerns were solicited, and if

not, why not; (3) whether Women-Owned Small Business concerns were solicited, and if not, why not; (4) whether HUBZone Small Business concerns were solicited, and if not, why not; (5) whether Veteran-Owned Small Business concerns were solicited, and if not, why not; (6) whether Service-Disabled Veteran-Owned Small Business concerns were solicited, and if not, why not; and (7) reasons for the failure of solicited concerns to receive the subcontract award.

D. Records of outreach efforts to contact trade associations, business development organizations and conferences and trade fairs to locate Small Businesses, and Native American Indian-Owned economic enterprises.

E. Records of internal guidance and assistance provided to Buyers through workshops, seminars, training, etc., and monitoring performance to evaluate compliance with Small Business Program requirements.

F. On a contract-by-contract basis, records to support award data submitted to the government or prime contractor, including the name, address and business size of each subcontractor.

G. Records of Small Business subcontracting plans for awards greater than $700,000 ($1,500,000 in the case of a contract for the construction of any public facility) and the Individual Subcontract Report where applicable.

H. The Harris GCS Small Business Program recognizes its Small Business suppliers with an annual awards ceremony for the “Outstanding Supplier of the Year” using supplier ratings, performance history, subcontract award information and procurement personnel input.

14.0 UTILIZATION OF PROPOSED SMALL BUSINESS SOURCES- FAR 52.219-9 (d)(12-13)

For small business suppliers in which Harris has identified in the proposal via a letter of intent or teaming agreement, Harris offers assurance that it will make a good faith effort to utilize those small business concerns, in the same or greater scope, amount, and quality used in preparing and submitting the bid or proposal.

Harris commits to provide written notification to the contracting officer of any failure to acquire articles, equipment, supplies, services or materials or obtain the performance of

construction work within thirty (30) days of contract completion.

15.0 SMALL BUSINESS- CONTRACTING OFFICER DISCUSSIONS- FAR 52.219-9 (d) (14)

Harris shall not prohibit a subcontractor from discussing any material matter pertaining to payment to or utilization of a subcontractor with the contracting officer.

16.0 TIMELY PAYMENTS TO SMALL BUSINESSES- FAR 52.219-9 (d) (15)

Harris shall pay its small business subcontractors on time and in accordance with the terms and conditions of the subcontract. Further, Harris assures that it will notify the contracting office of any reduced or untimely payments made to a small business subcontractor.

17.0 SMALL BUSINESS INNOVATION RESEARCH (SBIR)

Harris GCS has endorsed and supported SBIR technology efforts since ~ 2003. Support efforts were largely MDA related and resulted in some technology insertion into Harris systems. In 2010 Harris began interacting with the Air Force SBIR Commercialization Readiness Program technology integration meeting process culminating in Harris hosting its first technology interchange in GFY 2011 (October 2010). Subsequent technology interchange meetings were held in GFY 2012 (Nov 2-3, 2011), GFY 2013 (Nov 13-15, 2012), GFY 2014 (April 2-3, 2014) and GFY 2015 (Apr 29-30, 2015). Harris was recognized by the Air Force in March 2012 for its best practices in quickly adapting to the technology interchange meeting process producing one of the most successful workshops the Air Force and Navy experienced.

This strategic approach to matching technology gaps against potential SBIR developed technology solutions has been successful. SBIR technology is incorporated in Harris products *SeaLancet™ Network Radio* and *RedHawk™ Intuitive Haptic Control System*.

18.0 MENTOR-PROTÉGÉ & INFORMAL MENTORING

Harris is a dedicated proponent of establishing and maintaining Mentor-Protégé Agreements. Harris is a skilled mentor with expertise in a variety of areas, and fully aware of the importance of supporting small business, as well as providing expert guidance to them.

18.1 Formal Agreements

Harris GCS is an approved mentor in the National Geospatial-Intelligence (2011) and DoD (mid-1990s) Mentor-Protégé Programs. The types of developmental assistance provided to protégé firms under formal agreements includes: provision of accelerated QA tool for feature data extraction verification, user training and follow-on technical support; assistance with selection of image processing COTS application and user training on process fundamentals; quality & preproduction engineering; material and inventory planning; skills training; marketing communications; contract and financial management and planning; organizational management; overall business management and planning; business development; technical assistance and support; human resources assistance; security support; rent-free use of facilities and/or equipment.

18.2 Informal Mentoring

Harris has a best practice to engage in mentoring relationships with existing and potential Small Business suppliers and provide hands-on developmental assistance. This practice ensures that the Small Business is poised to provide a more comprehensive set of technical and professional services that will consistently exceed the expectations of Harris, the customers we serve and the customer base of the Small Business Concern. In time, it is envisioned that the Small Business will, by virtue of the Mentoring relationship, be mature enough to prime contracts and, team with and subcontract based on contract applicability.

Harris GCS hosts monthly meetings of the central & north Florida Minority Supplier Development Council (cnFMSDC) Space Coast chapter. Training and mentoring is provided by way of select topics and invited speakers designed to improve business and technical acumen. The Agenda includes a business spotlight provided by a large business for the benefit of networking, bringing opportunities to women/minority owned businesses in hopes they will grow and create jobs.

Separately, the Harris GCS Small Business Office educates program management, capture managers and business development personnel, through formal presentations and one-on-briefings, concerning the benefits to be gained and commitment involved in engaging in Mentoring relationships. This education has entailed providing the

requirements of differing U.S. Federal government agency programs, and the expected Protégé outcome based on the Mentor assistance to be provided.

19.0 PRIOR COMPLIANCE WITH OTHER SUBCONTRACTING PLANS

Harris GCS has been a participant of the DoD Comprehensive Small Business Subcontracting Plan - Test Program since 1996. Participation under the Comprehensive Subcontracting Program enables Harris GCS to focus its resources on increasing subcontracting opportunities for Small Business Concerns with a total division approach. Harris received a "Highly Successful" rating as a result of a Defense Contract Management Agency review of its 2014 Small Business Program.

(b) (2), (b) (4) [redacted]

20.0 DESCRIPTION OF GOOD FAITH EFFORT

Harris will measure performance against goals identified in Individual Small Business Subcontracting Plans and continuously evaluate our processes to encourage and improve Small Business participation. Harris understands that failure to comply in good faith with the clause of this contract titled "Utilization of Small, Business Concerns", or an approved plan required by this clause, shall be a material breach of the contract.

ATTACHMENT A: INDIVIDUAL SMALL BUSINESS SUBCONTRACTING PLAN GOALS

As described by Harris' Individual Subcontracting Plan, individual goals for Network Services 2020 **Enterprise Infrastructure Solutions (NS2020 EIS**) are indicated at Table 1.0. The total percentage of planned subcontracting with Small Business concerns includes total dollars planned to be subcontracted with Small (SB), Small Disadvantaged Business (SDB), Women-Owned Small (WOSB), HUBZone Small (HZSB), Veteran-Owned Small (VOSB) and Service-Disabled Veteran-Owned Small Business (SDVOSB). Given NS2020 EIS is an IDIQ contract and the potential contract value is not known,

(b) (2), (b) (4)

Table 1.0-1. NS2020 EIS Five Year Base Period Planned Subcontracting

Distribution	Base (5 Years)	% of Planned Subcontracting* (Subcontracting Goals)
Planned Contract Value	(b) (2), (b) (4)	
(b) (2), (b) (4)		

Table 1.0.2. NS2020 EIS Five Year Option 1 Planned Subcontracting

Distribution	Option 1 (5 Years)	% of Planned Subcontracting* (Subcontracting Goals)
Planned Contract Value	(b) (2), (b) (4)	
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		

Table 1.0-3. NS2020 EIS Five Year Option 2 Planned Subcontracting

Distribution	Option 2 (5 Years)	% of Planned Subcontracting* (Subcontracting Goals)
Planned Contract Value	(b) (2), (b) (4)	
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		

Table 1.0-4. NS2020 EIS Total (Base and Options) Planned Subcontracting

Distribution	Total (15 Years)	% of Planned Subcontracting* (Subcontracting Goals)
Planned Contract Value	(b) (2), (b) (4)	
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Indirect and overhead costs have not been included in the goals.

SIGNATURE REQUIRED:

This subcontracting plan was SUBMITT (b) (2), (b) (4)	**This subcontracting plan was EPTED by:**
Signature:	ature:
Typed Name: (b) (2), (b) (4)	d Name:
Title: (b) (2), (b) (4)	Title:
Date: (b) (2), (b)	Date:

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)

(b) (2), (b) (4)