L3HARRIS®
FAST. FORWARD.

Security for Land Mobile Devices

Secure Cloud-Based Radio Programming

L3Harris Technologies, Inc.

WHITE PAPER

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

Secure Radio Programming

SUMMARY

Cloud technologies and the Internet of Things (IoT) are a major transformation in the digital world that effects nearly everyone and every business today. These technologies offer flexibility, scalability, reliability, redundancy and greater economy of scale.

As critical communications systems interconnect with enterprise environments over the cloud, they must do so securely. Interoperability via the cloud typically increases an organization's risk exposure factor. For this reason, stringent cybersecurity controls are implemented using a Defense-in-Depth / Layered-Security strategy throughout the Device Management Framework (DMF).

Understanding the critical need for robust cybersecurity in Cloud and IoT systems, this white paper outlines the DMF security controls and capabilities designed to safeguard sensitive data and ensure system integrity. Readers will explore security measures based on trusted standards, including NIST 800-53 Rev. 5, DISA STIGs, and CIS Benchmarks, gaining insights into how these frameworks can strengthen their cybersecurity posture.

WHAT IS DMF?

The Device Management Framework (DMF) is a comprehensive solution designed to streamline the management and maintenance of IoT devices, particularly radio fleets, through a secure, cloud-based platform. It enables organizations to perform critical tasks such as firmware updates, feature installations, and real-time device monitoring without requiring devices to be removed from service. By leveraging a centralized online portal accessible via broadband connection, DMF ensures operational efficiency, reduces in-field technician time, and minimizes total cost of ownership (TCO). Additionally, it fortifies device security against emerging cyber threats and offers tiered support options, making it an adaptable and cost-effective choice for varying organizational needs. Built on principles of openness, adaptability, and reliability, DMF empowers users to maintain device performance and security effortlessly in dynamic operational environments.

SECURITY: STRATEGIES USED TO ENSURE SENSITIVE DATA AND SYSTEM INTEGRITY

Identity Federation

DMF uses Identity Federation through AWS Identity and Access Management (IAM) and Active Directory (AD) to centrally manage the identities for all L3Harris accounts across all applications/components of the DMF infrastructure to ensure only active employees in good standing can access DMF and to enforce uniformity of access control.

Authentication

DMF uses AWS Identity and Access Management (IAM) and Single Sign On (SSO) with Identity Federation to Active Directory (AD) to authenticate all L3Harris users. AWS multi-factor authentication (MFA) is also used via Azure AD to provide a second layer of authentication to L3Harris users before granting administrative access. Additionally, customer accounts are authenticated via AWS Cognito using strong password authentication. Tokens are returned by Cognito upon authentication and they are tied to AWS roles / policies granting specific / fine-grained level of access. Radios use X509 certificate authentication to authenticate against DMF.

Role-Based Access Control

DMF uses AWS roles and policies extensively to grant the appropriate level of access to users based on need-to-know. The principle of **separation of duties** is also used to avoid super-user accounts and require more than one user to perform certain administrative tasks to minimize fraud and error. The principle of **least privilege** is enforced on all roles to ensure only the minimal permissions that are required to perform a task are granted.

Session Management

DMF client sessions have automatic lock-out in place after a period of inactivity to protect against unauthorized access. Sessions are also terminated after a certain period of inactivity or upon user request.

Remote Access

All L3Harris remote administrative / privileged access requires multi-factor authentication (MFA) and separation of duties and least privilege.

Encryption In Transit

DMF uses the principle of **privacy by design** to treat all data in transit as sensitive and secure it. Only secure protocols are used to connect to the radios and infrastructure: HTTPS, MQTTS, SFTP, DTLS 1.2 and TLS 1.2. All data in transit is encrypted via AES-256.

Encryption At Rest

DMF uses the principle of Privacy by Design to treat all data at rest as sensitive and secure. All data at rest (S3 buckets, databases, files) is encrypted via AES-256. Hashes and digital signatures use SHA-2 or SHA-3.

Web Application Firewall (WAF)

All traffic to the DMF web client and Application Programming Interfaces (APIs) goes through an AWS Web Application Firewall (WAF) that provides protection against the Open Web Application Security Project (OWASP) Top 10 attacks and other web-based attacks.

API Gateway

DMF uses an AWS API Gateway service to authenticate requests and determine the request context to limit access to appropriate data. All API requests from the DMF web client are processed by the API Gateway.

Key Lifecycle Management

Key material used for encryption is stored/managed/rotated by the AWS Key Management Service (KMS). Separate keys are used for the logs and databases. Keys are rotated automatically annually.

Traffic Flow Control

DMF uses AWS Virtual Private Clouds (VPCs), Subnets and Security Groups to isolate traffic for public / private domains. VPCs and subnets segregate public and private domains. Security groups for the VPCs restrict inbound/outbound traffic at the IP/Port level.

Least Functionality

DMF uses the principle of least functionality, where only the needed functions, ports, services and protocols are used. Least functionality is checked via AWS Inspector, AWS Config. and Qualys Cloud Agent.

Centralized Logging and Monitoring

Centralized logging is performed via AWS CloudTrail. Security audit events are captured and logged to a centralized AWS S3 bucket that is under strict access control. All logging events use Universal Coordinated Time (UTC) time stamps and all components that are part of the DMF infrastructure use the Network Time Protocol (NTP) to coordinate their time. AWS CloudWatch is used to correlate and monitor the logs and generate alerts when there is a security event.

Center for Internet Security (CIS) Benchmarks

The Center for Internet Security (CIS) is a non-profit organization that defines benchmarks for Cyber Defense based on the knowledge and expertise of Cybersecurity and domain experts. DMF implements the CIS Benchmarks for:

- AWS
- Kubernetes
- Docker

Security Technical Implementation Guides (STIGS)

STIGS are a set of security requirements provided by the Defense Information System Agency (DISA) to secure hardware, software and infrastructure to reduce security vulnerabilities. DMF uses STIGS for operating systems, Java and other DMF infrastructure components.

Backup and Recovery

DMF uses incremental backups via built in AWS DynamoDB Point-In-Time-Recovery (PITR) automatic backup functionality to ensure mission critical data is always backed up and can be restored promptly in case of failure.

Secure Development Lifecycle (SDL)

DMF development follows SDL best practices of Static Application Security Testing (SAST) to identify weaknesses in code that can lead to security vulnerabilities, Software Composition Analysis (SCA) to identify security vulnerabilities in third-party components and libraries and Dynamic Application Security Testing (DAST). These best practices are performed as part of SecDevOps to perform continuous monitoring and identify and remediate security vulnerabilities on an ongoing basis.

DMF CYBERSECURITY CAPABILITIES

SECURITY REQUIREMENT	DESCRIPTIONS
Identification and Authentication	› Identity Federation via AWS IAM and AD for L3Harris accounts › MFA via AWS SSO and Azure AD for L3Harris administrators › Cognito strong password/token authentication for customers › Certificate based authentication for radios › API Gateway authentication for API requests
Access Control and Session Management	› Role-based Access Control (RBAC) › AWS Managed Roles with Least Privilege and Separation of Duties › AWS Policies for fine grained control › Remote Access via MFA for privileged L3Harris accounts › Session lockout after inactivity or upon user request › Session termination after inactivity or upon user request
Encryption	› Encryption in transit: TLS 1.2, DTLS 1.2, HTTPS, MQTTS, SFTP, AES-256 › Encryption at rest: AES-256 › Key lifecycle management through AWS KMS
Perimeter Security	› AWS Virtual Private Clouds to isolate domains › AWS Subnets to further isolate domains › AWS Security Groups to restrict traffic flow › AWS Web Application Firewall to protect the DMF client and APIs › AWS API Gateway to protect API calls
Security Baselines	› DISA STIGS for Operating Systems, Java and other DMF infrastructure components › CIS Benchmarks for AWS, Kubernetes and Docker › Least Functionality via AWS Inspector and Qualys CloudAgent
Centralized Logging and Monitoring	› Centralized logging to AWS S3 via AWS CloudTrail › Centralized Monitoring and alerting via AWS CloudWatch › UTC Time stamps for event correlation › Coordinated time via NTP for event correlation
Backup and Recovery	› Point-In-Time-Recovery (PITR) automatic backup functionality via DynamoDB
Secure Development Lifecycle	› Static Application Security Testing (SAST) to identify weaknesses in code › Software Composition Analysis (SCA) to identify vulnerabilities in 3rd party components › Dynamic Application Security Testing (DAST) to identify vulnerabilities in running code › SecDevOps to perform continuous monitoring/remediation

Table 1: Cybersecurity Controls

DMF Security White Paper

L3Harris Technologies is the Trusted Disruptor in the defense industry. With customers' mission-critical needs always in mind, our employees deliver end-to-end technology solutions connecting the space, air, land, sea and cyber domains in the interest of national security. Visit L3Harris.com for more information.

1025 W. NASA Boulevard
Melbourne, FL 32919

L3Harris.com