Alaska Land Mobile Radio Communications System

System Vulnerability Management Procedure 400-6

Version 8

October 11, 2016

Developed in conjunction with:

Bering Straits Information Technology, LLC
A Subsidiary of the Bering Straits Native Corporation

Table of Contents

Document Revision History

Name	Date	Reason for Changes	Version
Shafer, Sherry	5/4/2009	Approved by the User Council – Final.	1
Shafer, Sherry	5/24/1010	Annual review/update. Approved by the User Council – Final.	2
Shafer, Sherry	5/26/2011	Annual review/update. Approved by the User Council – final.	3
Shafer, Sherry	8/1/2012	Annual review/update. Approved by the User Council – final.	4
Shafer, Sherry	7/8/2013	Annual review/update. Approved by the Operations Management Office - final.	5
Shafer, Sherry	7/29/2014	Annual review/update. Approved by the Operations Management Office - final.	6
Shafer, Sherry	8/3/2015	Annual review/update. Approved by the Operations Management Office - final.	7
Shafer, Sherry	10/11/2016	Annual review. Approved by the Operations Management Office - final.	8

Acronyms and Definitions

Alaska Federal Executive Association (AFEA): federal government entities, agencies and organizations, other than the Department of Defense, that operate on the shared ALMR system infrastructure.

Alaska Land Mobile Radio (ALMR) Communications System: the ALMR Communications System, which uses but is separate from the State of Alaska Telecommunications System (SATS), as established in the Cooperative Agreement.

Alaska Municipal League: a voluntary non-profit organization in Alaska that represents member local governments.

Cybersecurity: Cybersecurity replaces and is synonymous with Information Assurance (IA) IAW Department of Defense Instruction (DoDI) 8500.01, *Cybersecurity*. Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Defense Information Systems Agency (DISA): the Defense Information Systems Agency is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war.

Department of Defense – Alaska: Alaskan Command, US Air Force and US Army component services operating under United States Pacific Command and United States Northern Command.

Executive Council: the ALMR Executive Council which is made up of three voting members and two associate members representing the original four constituency groups: the State of Alaska, the Department of Defense, Federal Non-DOD agencies (represented by the Alaska Federal Executive Association), and local municipal/government (represented by the Alaska Municipal League and the Municipality of Anchorage).

Information Assurance Vulnerability Alert (IAVA): Notification that is generated when an Information Assurance vulnerability may result in an immediate and potentially severe threat to DOD systems and information; this alert requires corrective action because of the severity of the vulnerability risk.

Local Governments: those Alaska political subdivisions defined as municipalities in AS 29.71.800(13).

Municipality of Anchorage (MOA): the MOA covers 1,951 square miles with a population of 300,000 plus. The MOA stretches from Portage, at the southern border, to the Knik River at the northern border, and encompasses the communities of Girdwood, Indian, Anchorage, Eagle River, Chugiak/Birchwood, and the native village of Eklutna.

Risk Management Framework (RMF) for DoD Information Technology (IT): A structured approach used to oversee and manage risk for an enterprise. The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. Requires the completion of the Assessment and Authorization (A&A), formerly certification and accreditation (C&A), process which results in an Authorization Decision (AD). The system must be reauthorized no later than every three (3) years.

Security Manager (SCM): the individual responsible for establishing and maintaining security controls that ensure the availability, confidentiality and integrity of the ALMR System.

Security Technical Implementation Guide (STIG): Based on Department of Defense (DOD) policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DOD baseline.

State of Alaska (SOA): the primary maintainer of the SATS (the State's microwave system), and shared owner of the System.

State of Alaska Telecommunications Systems (SATS): the State of Alaska statewide telecommunications system microwave network.

System Management Office (SMO): the team of specialists responsible for management of maintenance and operations of the System.

User Council: the User Council is responsible for recommending all operational and maintenance decisions affecting the System. Under the direction and supervision of the Executive Council, the User Council has the responsibility for management oversight and operations of the System. The User Council oversees the development of System operations plans, procedures and policies under the direction and guidance of the Executive Council.

1.0 Purpose

This policy applies to all System Management Office (SMO) employees, contractors, subcontractors, consultants, temporary employees and other personnel assigned to, or utilizing, the Alaska Land Mobile Radio (ALMR) Communications System.

In order to ensure the proper level of System integrity and availability is maintained, a regular assessment of ALMR systems shall be performed. This assessment will identify configuration vulnerabilities in the ALMR System and shall be used to dictate System vulnerability mitigation efforts.

2.0 Roles and Responsibilities

2.1 Executive Council

The Executive Council (EC) shall be responsible for the management and enforcement of sanctions when violations of the System Vulnerability Management Procedure warrant such action.

2.2 User Council

The User Council (UC) shall be responsible for the formal approval of the System Vulnerability Management Procedure, and any substantial revisions hereafter.

2.3 Security Manager

The Security Manager (SCM):

- Ensures this System Vulnerability Management Procedure sufficiently meets or exceeds the requirements for security standards based on a system with a Security Impact of Moderate Confidentiality, Moderate Integrity, and Moderate Availability.
- Regularly reviews and updates this procedure to ensure that all vulnerability management needs are documented and met
- Oversees the implementation of approved System configurations, as well as updates and patches
- Performs vulnerability assessments using approved third party tools in accordance with the vulnerability assessment schedule
- Ensures network assessments are performed and includes the appropriate vulnerability checks for all systems that comprise the ALMR network

2.4 System Management Office

2.4.1 The System Management Office (SMO) coordinates with System Technologists and the SCM to ensure that all required technical resources needed for regular vulnerability assessments and mitigation are available and implemented.

2.4.2 The SMO maintains a System Configuration Library, which details all ALMR information system configurations.

2.5 System Technologists

All System Technologists shall aid in the completion of vulnerability assessments, maintenance of a System Configuration Library and the mitigation of identified vulnerabilities.

3.0 Vulnerability Assessments

3.1 Frequency

A network Vulnerability Assessment shall be performed by the SCM at least quarterly. Assessment results must provide Information Assurance Vulnerability Alert (IAVA) compliant assessments. These assessments ensure any vulnerabilities found are addressed to ensure IAVA compliance for all ALMR network components.

3.2 Report

The SCM shall provide a report detailing the results of the quarterly vulnerability assessment scan to the Operations Manager. This report shall include, at a minimum:

- Detailed description of all vulnerabilities found
- Assessment of System impact for each vulnerability
- Recommended mitigation procedures

3.3 Review

The Operations Manager shall review the Vulnerability Assessment Reports to ensure proper attention is being given to ALMR System vulnerability mitigation.

4.0 Updates and Patches

4.1 Automated Updates

4.1.1 Automated update procedures should be used when available and appropriate.

4.1.2 Updates/patches to major system components should be preceded by a System backup. When System resources permit, updates/patches should be installed on a test system and monitored for undesirable results before being implemented in the production environment. (**NOTE:** This will typically be performed by the System manufacturer.)

4.2 Documentation

4.2.1 The SMO shall maintain, as a component of the System Configuration Library, documentation of current versions and patches applied on all software/hardware components of the ALMR System.

4.2.2 This document shall be used as the minimum version level requirement for new information systems that are to be connected to the ALMR System network.

5.0 System Configuration Management

5.1 System Configuration Library

The SMO shall maintain a detailed library of configuration instructions for all ALMR Information Systems. The maintenance of this library should be a collective effort of all ALMR System Technologists, the System Manager, SCM and the System Manufacturer (Motorola™).

5.2 Replacement/New Hardware Configuration

Detailed instructions describing the process to configure replacement or new hardware will be maintained in the library. These instructions shall be followed during System replacement/installation to preclude the introduction of vulnerabilities through improper System configuration.

6.0 Vulnerability Remediation

Remediation of network vulnerabilities found on the ALMR System should be performed in accordance with Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), Information Assurance Vulnerability (IAV) Bulletins and industry standards. Third party tools and workarounds used to remediate vulnerabilities should be avoided unless their use is specifically recommended by DISA STIGs, IAV Bulletins or industry standards.

6.1 Remediation Prioritization

The ALMR System has two priority levels for vulnerability remediation, as defined by the SCM.

6.1.1 Level 1 Vulnerabilities. Vulnerabilities with a prioritization of Level 1 are vulnerabilities classified as 'High' or 'Medium' and found on ALMR components that physically reside in one of the following locations:

- Zone 1 Master Site
- Zone 2 Master Site
- All Remote Repeater Sites

6.1.2 Level 2 Vulnerabilities. Vulnerabilities with a prioritization of Level 2 are vulnerabilities classified as 'Low' and found on ALMR components that physically reside in one of the following locations:

- Zone 1 Master Site
- Zone 2 Master Site
- All Remote Repeater Sites
- Any User Controlled System (Console, KMF PC, KMF Server, etc.)

or

Vulnerabilities classified as 'High' or 'Medium' and found on ALMR components that physically reside in:

- Any User Controlled System (Console, KMF PC, KMF Server, etc.)

6.2 Remediation Schedule

6.2.1 Level 1 Vulnerabilities

All Level 1 vulnerabilities should be mitigated within 30 days of discovery. In the event that a Level I vulnerability cannot be mitigated within the 30-day limit, the SCM shall ensure a detailed mitigation report is included in the Vulnerability Assessment Report provided to the Operations Manager.

6.2.2 Level 2 Vulnerabilities

All Level 2 vulnerabilities should be mitigated within 90 days of discovery. In the event that a Level 2 vulnerability cannot be mitigated within the 90-day limit, the SCM shall ensure a detailed mitigation report is included in the Vulnerability Assessment Report provided to the Operations Manager.

7.0 Compliance

Compliance with the System Vulnerability Management Procedure is outlined in ALMR System Vulnerability Management Policy Memorandum 400-6.