Alaska Land Mobile Radio Communications System

Information Systems Clearing and Sanitization Procedure 200-4

Version 9

August 31, 2016

Developed through contract 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	4/28/2008	Final	1
Shafer, Sherry	4/17/2009	Annual review/update. Approved by the User Council – final.	2
Shafer, Sherry	5/3/2010	Annual review/update. Approved by the User Council - final.	3
Shafer, Sherry	5/26/2011	Annual review/update. Approved by the User Council - final.	4
Shafer, Sherry	9/19/2012	Annual review/update. Approved by the User Council - final.	5
Shafer, Sherry	9/3/2013	Annual review/update; approved by the OMO - final.	6
Shafer, Sherry	9/15/2014	Annual review/update. Approved by the Operations Management Office – final.	7
Shafer, Sherry	9/9/2015	Annual review/update. Approved by the User Council - final.	8
Shafer, Sherry	8/31/2016	Annual review/update. Approved by the Operations Management Office – final.	9

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 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.

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).

Impact: The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.

Impact Level: The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

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.

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/Member: an agency, person, group, organization or other entity which has an existing written Membership Agreement with one of the Parties to the Agreement. The terms user and member are synonymous and interchangeable.

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 operation 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

To establish controls to ensure Alaska Land Mobile Radio (ALMR) Communications System documents, equipment and machine-readable media are properly cleared, sanitized and decommissioned, when appropriate. Failure to follow this procedure will put ALMR at risk of unauthorized disclosure of proprietary or sensitive information, legal issues and potential Denial of Authority to Operate (DATO) under the Risk Management Framework (RMF) for DoD Information Technology (IT), known as RMF.

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 Information Systems Clearing and Sanitization Procedure warrant such action.

2.2 User Council

The User Council (UC) shall be responsible for the formal approval of the Information Systems Clearing and Sanitization Procedure and any substantial revisions hereafter.

2.3 System Management Office

The System Management Office (SMO) is responsible for ensuring that all documents, equipment and machine-readable media assets, which contain information on or utilize memory of any type, are cleared and sanitized before reuse or decommissioning in accordance with this procedure.

To ensure the proper level of clearing and sanitization of ALMR assets occurs, the SMO shall ensure all personnel authorized to perform clearing, sanitization and decommissioning are properly trained and aware of the applicable directives, policies and procedures.

2.4 Security Manager

The Security Manager (SCM) shall develop, disseminate and periodically review/update formal, documented procedures to facilitate the proper security of ALMR System components by ensuring all documents, equipment and machine-readable media is cleared or sanitized.

The SCM shall also assign security priorities and approve security standards based on the required Security Controls for system security impact levels of **Low** confidentiality,

Moderate Integrity and **Moderate** Availability, thereby maintaining visibility over all clearing and sanitizing policy assignments.

ALMR has security impact levels of **Low** confidentiality, **Moderate** Integrity and **Moderate** Availability and must be protected accordingly.

2.5.1 User Agencies

User agencies shall follow the same standards for clearing, sanitizing and decommissioning all agency-owned documents, equipment and machine-readable media assets containing information on or having been connected to the ALMR System.

3.0 Clearing

Clearing is the process of eradicating data on equipment and media before retiring the equipment or reusing the media. This includes media such as internal memory, video memory, caches, recovery partitions, buffers or other forms of reusable memory. This process ensures that unauthorized access to previously stored information is denied or that the information is no longer readable by any known method.

3.1 Master Site Hardware and Software

All ALMR System components at the Master Sites at Tudor Road and Birch Hill possess the highest value in terms of cost and System reliance. When scheduled for re-assignment or decommission, each ALMR asset located at a master or secondary site shall have every addressable memory location overwritten with a single character or the physical storage media must be destroyed. The method of destruction must preclude recognition or reconstruction of the information or material. This action must be performed by an authorized employee of the SMO, and a record of the destruction documentation forwarded to the ALMR Asset Manager along with a copy of the Service Request.

3.2 Consoles

Similar to the master site assets, when scheduled for re-assignment or decommission, each ALMR console shall have every addressable memory location overwritten with a single character or the physical storage media must be destroyed. The method of destruction must preclude recognition or reconstruction of the information or material. This action can be performed by the owner of the equipment or the SMO, but a record of the destruction documentation must be forwarded to the ALMR Asset Manager for record keeping.

3.3 Cryptographic Key Variable Loaders

Every ALMR key variable loader (KVL), regardless of location, shall be closely monitored and audited for use. The SMO shall document the number of key programmers, their serial numbers and status (deployed, under repair, decommissioned, etc.). These audits should be maintained in a way that is secure and in accordance with ALMR Records Management processes and procedures and immediately available for inspection, upon request.

The most valuable function of the KVL is the algorithm in each device, which cannot be cleared or sanitized. The keys maintained on these assets must be wiped in a manner whereby no internal media can be deciphered. The only known way to ensure the loader's algorithm cannot be compromised once it has left the control of ALMR is to physically destroy it.

Any ALMR personnel responsible for a KVL must immediately report to the ALMR Help Desk when a KVL is unaccounted for either through theft or loss. The Help Desk will notify the SCM and the Asset Manager.

3.4 Subscriber Units

All pre-existing cryptographic keys or configurations shall be cleared, or zeroed out, in a manner which prohibits the radio from having access to the ALMR System voice network, before being sent to maintenance or prepared for decommissioning.

It is the responsibility of each agency to clear cryptographic keys and configurations before a subscriber unit is sent for maintenance or decommissioned. User agencies shall provide written notification of subscriber units being decommissioned to the SMO. Written notification shall be sent via email to the ALMR Help Desk.

For assistance regarding the proper clearing of cryptographic keys and configurations on a subscriber unit, agencies should contact the ALMR Help Desk.

4.0 Sanitization

All ALMR systems shall undergo a process to remove sensitive data before any reuse of such systems in another environment that does not provide an acceptable level of protection for ALMR data.

4.1 Maintenance Personnel and Repairs

The time when ALMR System assets are most vulnerable to exploitation is during system maintenance. Security awareness of the maintenance personnel and their access to sensitive information shall be clearly known to the SCM prior to approval.

If appropriately cleared personnel, as defined by the SCM, are unavailable to perform maintenance or repair, personnel with a lesser clearance may be used, but only under escort and monitored by approved ALMR personnel, as defined by the SCM.

4.2 Decommissioning

Once an ALMR computing asset is targeted to be replaced or discarded as a result of defect or product enhancement, each asset must be properly cleared and sanitized and its status annotated by the Asset Manager. These actions must be documented in the form of a report. These reports shall be maintained in a manner consistent with ALMR Records Management Procedure 300-1.

5.0 Compliance

Compliance with the Information Systems Clearing and Sanitization Procedure is outlined in ALMR Information Systems Clearing and Sanitization Policy Memorandum 200-4.