



A FEDERAL, STATE AND MUNICIPAL PARTNERSHIP

Alaska Land Mobile Radio Communications System

Information Systems Clearing and Sanitization Procedure 200-4

Version 4

May 26, 2011

Developed through contract with:



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



Table of Contents

Table of Contents	i
Document Revision History	ii
Acronyms and Definitions	iii
1.0 Purpose	1
2.0 Roles and Responsibilities	1
2.1 Executive Council	1
2.2 User Council	1
2.3 System Management Office	1
2.4 Security Manager	1
2.5 Information Assurance Officer (IAO)	Error! Bookmark not defined.
3.0 Clearing	2
3.1 Master Site Hardware and Software	2
3.2 Consoles	2
3.3 Cryptographic Key Loaders	2
3.4 Subscriber Units	3
4.0 Sanitizing	3
4.1 Maintenance Personnel & Repairs	3
4.2 Decommissioning	4
5.0 Compliance	4



*Alaska Land Mobile Radio Communications System
Information Systems Clearing and Sanitization Procedure 200-4*

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



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.

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

Department of Defense Information Assurance Certification and Accreditation Process (DIACAP): established process that helps users and information security officers ensure information systems operate at an acceptable level of risk. As defined in interim guidance contained in Department of Defense Directive 8500.1, Information Assurance (IA), October 24, 2002, and DODI 8500.2, Information Assurance (IA) Implementation, February 6, 2003.

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, Non-DOD Federal 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 (IA): information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

IAO: Information Assurance Officer

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

Mission Assurance Category (MAC): mission category used to determine requirements and availability of information systems

Municipality of Anchorage (MOA): the MOA covers 1,951 square miles with a population of approximately 278,000. The MOA stretches from Portage, at the southern



*Alaska Land Mobile Radio Communications System
Information Systems Clearing and Sanitization Procedure 200-4*

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.

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 machine-readable media are properly cleared and sanitized. Failure to follow this procedure will put ALMR at risk of unauthorized disclosure of proprietary or sensitive information, legal issues, and potential Denial of Authorization to Operate (DATO) under the Department of Defense (DOD) Information Assurance Certification and Accreditation Process (DIACAP). Formal documentation shall exist regarding the steps taken to clear and sanitize all machine-readable media to deny access to previously stored information on ALMR computing assets.

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 Policy and 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 revisions hereafter.

2.3 System Management Office

The System Management Office (SMO) is responsible for ensuring that all machine-readable media assets, which utilize memory of any type, are cleared and sanitized 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 and sanitization are properly trained and aware of the applicable directives, policies, and procedures.

2.4 Security Manager

The Information Assurance Officer (IAO)/Security Manager shall develop, disseminate, and periodically review/update formal, documented procedures to facilitate the implementation of properly securing ALMR System components by ensuring all machine-readable media is cleared or sanitized.

The IAO shall also assign security priorities and approve security standards based on Mission Assurance Category II – Mission Essential, maintaining visibility over all clearing and sanitizing policy assignments.



Alaska Land Mobile Radio Communications System Information Systems Clearing and Sanitization Procedure 200-4

MAC II systems handle information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. These consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness.

A Mission Essential information system is a system that meets the definition of “information system” IAW Chapter 25, Title 40 United States Code, that the acquiring component head or designee determines what is basic and necessary for the accomplishment of organizational mission.

ALMR is considered a MAC II system and must be protected accordingly.

3.0 Clearing

Clearing is the process of eradicating data on media before reusing the media. This includes media such as internal memory, buffer, 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

When scheduled for repair or decommission, every ALMR console, regardless of location, shall have every addressable memory location overwritten with a single character. Additionally, these assets must be degaussed applying coercivity greater than 750 oersteds. This action must be performed by an authorized employee of the ALMR SMO.

3.3 Cryptographic Key Loaders

Every ALMR key loader, 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). These audits should



Alaska Land Mobile Radio Communications System Information Systems Clearing and Sanitization Procedure 200-4

be maintained in a way that is secure and in accordance with ALMR Records Management procedures, and immediately available for inspection, when required.

The most valuable function of the key loader 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 key programmer must immediately report to the ALMR Help Desk when a key loader is unaccounted for either through theft or loss. The Help Desk will notify the IAO/Security Manager and the Asset Manager.

3.4 Subscriber Units

All pre-existing cryptographic key or configurations shall be cleared, or zeroed out, in a manner which prohibits the radio 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 Help Desk.

4.0 Sanitizing

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 IAO/Security Manager prior to approval.

If appropriately cleared personnel, as defined by the IAO/Security Manager 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 IAO/Security Manager.



Alaska Land Mobile Radio Communications System Information Systems Clearing and Sanitization Procedure 200-4

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.