Alaska Land Mobile Radio Communications System

Cybersecurity Procedure 200-5

Version 10

July 20, 2017

Developed through contract with:

Table of Contents

Document Revision History

Name	Date	Reason for Changes	Version
Huls, Chad	5/13/2008	Approved by User Council – Final.	1
Shafer, Sherry	6/8/2009	Annual review/update. Approved by the User Council – Final.	2
Shafer, Sherry	7/7/2010	Annual review/update. Approved by the User Council – Final.	3
Shafer, Sherry	8/4/2011	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
Bohman, Andreas Shafer, Sherry	4/24/13 5/14/2013	Out of cycle review; requested change by the Security Manager to add Security Technician to training record maintenance. OMO/SMO review. Approved by the User Council - final.	6
Shafer, Sherry	6/2/2014	Annual review/update. Approved by the Operations Management Office - final.	7
Shafer, Sherry	6/29/2015	Annual review/update. Approved by the Operations Management Office - final.	8
Shafer, Sherry	7/19/2016	Annual review. Approved by the User Council - final.	9
Shafer, Sherry	7/20/2017	Annual review/update. Approved by the Operations Management Office - final.	10

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: 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 Administration (DOA): a State of Alaska (SOA) department that maintains the SOA Telecommunication System (SATS) and provides information technology (IT) and communications technical support to state agencies.

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).

Federal Information Security Management Act of 2002 (**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 was meant to bolster computer and network security within the federal government and affiliated parties (such as government contractors) by mandating yearly audits.

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).

Member: a public safety agency including, but not limited to, a general government agency (local, state or federal), its authorized employees and personnel (paid or volunteer), and its service provider, participating in and using the System under a Membership Agreement.

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.

Operations Management Office (OMO): develops recommendations for policies, procedures, and guidelines; identifies technologies and standards; and coordinates intergovernmental resources to facilitate communications interoperability with emphasis on improving public safety and emergency response communications.

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 Technician: holds a Security+ certification and provides services at the direction of the Security Manager, which may include, but are not limited to, dissemination of the Cybersecurity Awareness Program, signing training certificates and maintenance of training records for all System users.

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 to operate on ALMR with one of the Parties to the Cooperative 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 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.

NOTE: The term "Information Assurance" will continue to be used in reference documents until such time as existing Department of Defense Directives/ Instructions/Manuals are revised to update the terminology to "Cybersecurity." The difference in terms **does not** change the directive nature of such documents. For all intended purposed, the terms are to be considered interchangeable and both maintain the full force of the law, as such.

1.0 Purpose

Cybersecurity applies to all member agencies, employees, contractors, subcontractors, consultants, temporary employees and other personnel assigned to and/or utilizing the Alaska Land Mobile Radio (ALMR) Communications System equipment including hardware, firmware and software. This document defines user levels in accordance with Department of Defense Instruction (DODI) 8140.01, *Cyberspace Workforce Management*, for the identification of appropriate System user training.

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 Cybersecurity Procedure warrant such action.

2.2 User Council

The User Council (UC) shall be responsible for the formal approval of the Cybersecurity Procedure and any revisions hereafter.

2.3 Security Manager

The Security Manager shall oversee the creation and dissemination of the ALMR Cybersecurity Program. The Security Manager shall ensure that the program meets or exceeds the Cybersecurity Awareness training requirements set forth in DOD 8570.01-M.

2.4 Operations Management Office

The Operations Management Office (OMO) shall ensure that all users/agencies are aware of, and abide by, applicable ALMR policies, procedures, programs, etc., and shall make all related documents readily available to all users/agencies.

2.5 System Management Office

The System Management Office (SMO) shall:

- Implement and provide technical and managerial support to member agencies for all approved Cybersecurity requirements
- Develop training to satisfy the Cybersecurity training requirements for ALMR
- Disseminate training requirements, due dates and expectations to all user agencies
- Provide a web-based training environment for Level II and III users
- Track and review all Level II and III System users to ensure that each Level II and III user possesses a current training certificate
- Annually review the training content to verify applicability and update, as needed

2.6 User Agencies

2.6.1 System users shall be knowledgeable of, and comply with, all Cybersecurity applicable policies. Examples of ALMR policies that directly relate to Cybersecurity include:

- Information Systems Clearing and Sanitization Policy 200-4
- System Recovery Policy 400-1
- System Incident Response Policy 400-2
- System Account Control Policy 400-4

2.6.2 All System member agencies shall provide the SMO with a list of users who require Level II or Level III User Access, as outlined in paragraph 3. Member agencies will ensure the list is kept up to date and that each user has completed the appropriate level of Cybersecurity training no later than the annual due date.

3.0 System User Levels

3.1 Level I

3.1.1 Level I System users are defined as any employee, contractor, subcontractor, consultant, temporary employee or other personnel assigned to and/or utilizing the ALMR System. Level I System users include, but are not limited to:

- Portable and mobile subscriber unit operators
- System maintenance staff
- Members of the ALMR User Council

3.1.2 Level I System users must receive initial Cybersecurity Awareness orientation training. The DOD mandated Cyber Awareness Challenge located at http://iatraining.disa.mil/eta/cyberchallenge_v4/launchPage.htm must be completed annually. This training shall be a condition of access to, or use of, the ALMR System. Additional awareness training can be provided in classroom, computer-based or blended formats under the guidance of the ALMR Security Manager.

3.1.3 By the end of Cybersecurity Awareness orientation, a Level I System user should be able to:

- Understand acceptable use of the ALMR System
- Recognize a potential security violation
- Take appropriate action to report the incident
- Apply instructions and pre-established guidelines to perform Cybersecurity tasks

3.2 Level II

3.2.1 Level II System users provide network and computing environment support for the ALMR System. ALMR personnel within this level possess specialized technical experience and are in a position to identify System intrusions and System vulnerabilities.

3.2.2 Level II System users include, but are not limited to:

- Console operators
- Key Management Facility (KMF) managers
- Designated points of contact (POCs) for a member agency

3.3 Level III

3.3.1 Level III System users focus specifically on the ALMR enclave environment and are assigned to support, monitor, and test and troubleshoot Cybersecurity-related issues associated with the ALMR System. Level III System users have demonstrated mastery of all subject matter defined under Levels I and II.

3.3.2 Level III System users include:

- SMO technicians
- System administrators
- Database administrators
- ALMR maintenance staff
- Firewall administrators
- Security operations staff
- ALMR Security Manager

3.3.3 Individuals indentified by the ALMR Security Manager shall either possess a certification or be capable of being certified by a DOD-approved accrediting body at an Information Assurance Technical Level III (IAT III). IAT Level III approved accrediting bodies are defined under Table AP3.T1 of DOD 8570.01-M, Department of Defense Information Assurance Workforce Improvement Program.

4.0 Training Requirements

4.1 New Users

All new users are required to complete the appropriate level of training before they are granted access to the ALMR System. To request new user access and training, the member agency POC shall contact the ALMR Help Desk and initiate a New User Access Request.

4.2 Annual Training Review

All ALMR System users are required to renew their training certificate yearly in an effort to ensure the appropriate level of Cybersecurity Awareness is maintained by all personnel.

All training is tracked in a data base which is monitored and updated by the SMO.

5.0 Training Content

5.1 Level I Content

Level I System user Cybersecurity Awareness orientation training should include, at a minimum, the following topics as they apply to the ALMR System:

- What Cybersecurity is, and why it is necessary
- Physical security
- Acceptable use of the System
- Basic functionality orientation
- Security violation reporting and response procedures
- Rules and regulations
- Compliance

5.2 Level II Content

Level II System user training should include, at a minimum, the following topics as they apply to the ALMR System:

- Level I System Cybersecurity Awareness orientation training
- Risk Management Framework (RMF) for DOD Information Technology and Federal Information Security Management Act (FISMA) orientation
- System access control
- System user account management
- Password management
- Basic System maintenance

- Security violation reporting and response procedures
- Explanation of applicable policies and procedures

5.3 Level III Content

Level III System user training should assume an understanding of Level I and II training, as well as ensure a user's capability to:

- Recommend and schedule Cybersecurity-related repairs
- Lead teams to quickly solve Cybersecurity-related issues
- Determine if a security incident is a violation of ALMR policy, or relevant laws
- Monitor and evaluate the effectiveness of the Cybersecurity procedures and safeguards
- Analyze Information Assurance Vulnerability Alert (IAVA) reports and be able to understand the risk associated with each IAVA
- Provide on-the-job training for Level I and II System users
- Establish enclave logging procedures
- Schedule and perform special backups
- Design and maximize the functionality of perimeter defense including firewalls and intrusion detection systems
- Disaster Recovery

5.4 Training Records

The Security Manager or Security Technician shall maintain training records for all System users, which note each individual user's employment agency and training level status, at a minimum.

The Security Manager shall advise the UC if, and when, certification credentials have expired, been suspended, or forfeited.

The UC shall determine appropriate actions (including potential recertification) in the event of an expiration or suspension. The UC shall keep the EC updated on such events and make recommendation if further actions are warranted.

6.0 Compliance

Compliance with the Cybersecurity Procedure is outlined in ALMR Cybersecurity Policy Memorandum 200-5.

Reference Documents

1. Committee on National Security Systems Instruction (CNSSI) 4009, Committee on National Security Systems (CNSS) Glossary
https://www.cnss.gov/CNSS/openDoc.cfm?16JKx6BCaIIz+bNvAYLG4A

2. CNSSI 1253, *Security Categorization and Control Selection for National Security Systems*
https://www.cnss.gov/CNSS/openDoc.cfm?SQ+OVYk/ailg9GQSam+dWg

3. DODI 8144.01, Cyberspace Workforce Management,
http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf

4. DODI 8500.01, *Cybersecurity*,
http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

5. DODI 8510.01, *Risk Management Framework (RMF) for DOD Information Technology*
http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

6. DOD Manual 5200.01 Volume 4, *DOD Information Security Program: Controlled Unclassified Information (CUI)*
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf

7. DOD 8570.01-M, *Information Assurance Workforce Improvement Program,*
http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

8. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems And Organizations*
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf