ALASKA LAND MOBILE RADIO

Alaska Land Mobile Radio Communications System

Cybersecurity Procedure 200-5

Version 18

August 1, 2025

Developed through contract with:

Bering Straits Information Technology, LLC

A Subsidiary of the Bering Straits Native Corporation

Table of Contents

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 Information Systems Security Manager 1
2.4 Operations Management Office 1
2.5 System Management Office 2
2.6 User Agencies 2
3.0 System User Levels **2**
3.1 Level I 2
3.2 Level II 3
4.0 Training Requirements **4**
4.1 New Users 4
4.2 Annual Training Review 4
5.0 Training Content **4**
5.1 Level I Content 4
5.2 Level II Content 5
5.3 Training Records 5
6.0 Compliance **5**
Reference Documents **6**

Document Revision History

Date	Reason for Changes	Version
5/13/2008	Approved by User Council – Final.	1
6/8/2009	Annual review/update. Approved by the User Council – Final.	2
7/7/2010	Annual review/update. Approved by the User Council – Final.	3
8/4/2011	Annual review/update; approved by the User Council - final.	4
9/19/2012	Annual review/update; approved by the User Council - final.	5
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
6/2/2014	Annual review/update. Approved by the Operations Management Office - final.	7
6/29/2015	Annual review/update. Approved by the Operations Management Office - final.	8
7/19/2016	Annual review. Approved by the User Council - final.	9
7/20/2017	Annual review/update. Approved by the Operations Management Office - final.	10
7/17/2018	Annual review/update. Approved by the Operations Management Office - final.	11
8/14/2019	Annual review/update. Approved by the Operations Management Office - final.	12
8/27/2020	Annual review/update. Approved by the Operations Management Office - final.	13
8/26//2021	Annual review/update. Approved by the Operations Management Office - final.	14
8/9/2022	Annual review/update. Approved by the Operations Management Office - final.	15
8/3/2023	Annual review/update. Approved by the Operations Management Office - final.	16
8/12/2024	Annual review/update. Approved by the Operations Management Office - final.	17
8/1/2025	Annual review/update. Approved by the Operations Management Office – final.	18

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, as established in the Cooperative and Mutual Aid Agreement.

Alaska Municipal League: a voluntary non-profit organization in Alaska that represents 165 cities, boroughs, and unified municipalities.

Alaska Public Safety Communication Services (APSCS): a State of Alaska (SOA) office in the Department of Public Safety (DPS) that operates and maintains the SOA Telecommunications System (SATS) supporting ALMR and providing public safety communication services and support to state agencies.

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

Department of Public Safety (DPS): a State of Alaska (SOA) department where the SOA Telecommunications System (SATS) and ALMR programs reside.

Executive Council: governing body 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 Modernization Act of 2014 (**FISMA**)**:** a United States federal law enacted in December 2014, (Pub. L.113-283). The Act directs agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General Office (GAO). The Act requires such reports to include: (1) threats and threat actors, vulnerabilities, and impacts; (2) risk assessments of affected systems before and the status of compliance of the systems at the time of the major incidents; (3) detection, response, and remediation actions; (4) the total number of incidents; and (5) a description of the number of

individuals impacted and the information exposed by major incidents involving a breach of personally identifiable information.

Information Assurance Vulnerability Alert (IAVA): a 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.

Information Systems Security Manager (ISSM): the individual responsible for establishing and maintaining security controls that ensure the availability, confidentiality, and integrity of the ALMR system under the RMF.

Local Governments: those Alaska political subdivisions defined as municipalities in AS 29.71.800(14).

Member: a public safety agency including, but not limited to, a general government agency (local, state, tribal, 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 over 300,000. 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 manage information security risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (1) establishing the context for risk-related activities; (2) assessing risk; (3) responding to risk once determined; and (4) monitoring risk over time. The program 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 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 Information Assurance Awareness Program, signing training certificates, and maintaining training records for all system users.

State of Alaska (SOA): the primary maintainer of the State's infrastructure system, and shared owner of the system. The State of Alaska sponsors local/municipal agencies onto the system.

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

User: 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 and Mutual Aid Agreement. The terms user and member are synonymous and interchangeable. All terms and conditions of the Cooperative and Mutual Aid agreement defined apply to local/municipal government agencies that are sponsored/represented by the State of Alaska.

User Council: governing body 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.

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 purposes, 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 substantial revisions hereafter.

2.3 Information Systems Security Manager

The Information Systems Security Manager (ISSM) shall oversee the creation and dissemination of the ALMR Cybersecurity Program. The ISSM shall ensure that the program meets or exceeds the Cybersecurity Awareness training requirements set forth in DoD 8140.03.

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.
- Identify ISSM-approved Defense Information Systems Agency (DISA) web-based training environment for Level I and II users.
- Track and review all Level I and II system users to ensure that each Level I and II 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 I or Level II 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. Agencies shall ensure that all agency personnel utilizing subscriber units are familiar with and comply with the agency and ALMR policies and procedures regarding subscriber use and security.

3.0 System User Levels

3.1 Level I

3.1.1 Level I system users provide network and computing environment support for the ALMR system. ALMR personnel within this level possess specialized technical experience or maintain user accounts on ALMR assets and can identify system intrusions and system vulnerabilities.

- Console operators
- Key Management Facility (KMF) managers

- Designated points of contact (POCs) for a member agency

3.1.2 Level I system users must receive initial Cybersecurity Awareness orientation training. The DoD-mandated Cyber Awareness Challenge, located at https://public.cyber.mil/training/cyber-awareness-challenge/, 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 ISSM.

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 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 II system users have demonstrated mastery of all subject matter defined under Levels I and II.

3.2.2 Level II system users include:

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

3.2.3 Individuals identified by the ALMR ISSM shall either possess an Information Assurance Training (IAT) Level III certification or obtain a certification within one calendar year of being identified. Approved accrediting bodies and certifications are found in DoD Manual 8140.03 *Cyberspace Workforce Qualification and management Program.*

4.0 Training Requirements

4.1 New Users

All new users must 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 to ensure the appropriate level of Cybersecurity Awareness is maintained by all personnel.

All training is tracked in an Excel® spread sheet 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
- 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

5.2 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.
- 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.

5.3 Training Records

The ISSM 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 ISSM shall advise the User Council (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 Executive Council (EC) updated on such events and make recommendations 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 8140.03 *Cyberspace Workforce Qualification and Management Program.*
https://www.dodemergingtech.com/dod-programs/dod-8140/

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