



---

A FEDERAL, STATE AND MUNICIPAL PARTNERSHIP

---

# Alaska Land Mobile Radio Communications System

## Information Assurance Awareness Procedure 200-5

Version 4

August 4, 2011

Developed through contract with:



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



## **Table of Contents**

|   |            |
|---|------------|
| <b>Table of Contents</b> .....                | <b>i</b>   |
| <b>Document Revision History</b> .....        | <b>ii</b>  |
| <b>Acronyms and Definitions</b> .....         | <b>iii</b> |
| <b>1.0 Purpose</b> .....                      | <b>1</b>   |
| <b>2.0 Roles and Responsibilities</b> .....   | <b>1</b>   |
| 2.1 Executive Council (EC) .....              | 1          |
| 2.2 User Council (UC) .....                   | 1          |
| 2.3 Information Assurance Officer (IAO) ..... | 1          |
| 2.4 System Management Office (SMO) .....      | 1          |
| 2.5 ALMR User Agencies.....                   | 2          |
| <b>3.0 System User Levels</b> .....           | <b>2</b>   |
| 3.1 Level I .....                             | 2          |
| 3.2 Level II .....                            | 3          |
| 3.3 Level III .....                           | 3          |
| <b>4.0 Training Requirements</b> .....        | <b>3</b>   |
| 4.1 New Users .....                           | 3          |
| 4.2 Yearly Training Review .....              | 4          |
| <b>5.0 Training Content</b> .....             | <b>4</b>   |
| 5.1 Level I Content.....                      | 4          |
| 5.2 Level II Content.....                     | 4          |
| 5.3 Level III Content.....                    | 4          |
| 5.4 Training Records.....                     | 5          |
| <b>6.0 Compliance</b> .....                   | <b>5</b>   |
| <b>Reference Documents</b> .....              | <b>6</b>   |



## Document Revision History

| <b>Name</b>    | <b>Date</b> | <b>Reason for Changes</b>                                   | <b>Version</b> |
|----------------|-------------|---|----------------|
| 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              |
|                |             |   |                |
|                |             |   |                |
|                |             |   |                |



## **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.

**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).

**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 (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

**IAVA:** Information Assurance Vulnerability Alert

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



*Alaska Land Mobile Radio Communications System  
Information Assurance Awareness Procedure 200-5*

**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 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.

**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.

## **1.0 Purpose**

Information Assurance (IA) Awareness applies to all employees, contractors, consultants, temporary employees, and other personnel assigned to utilize 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) 8570.1, Information Assurance (IA) Training, Certification, and 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 Information Assurance Awareness Policy and Procedure warrant such action.

### **2.2 User Council**

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

### **2.3 Information Assurance Officer/Security Manager**

The Information Assurance Officer (IAO)/Security Manager shall oversee the creation and dissemination of the ALMR Information Assurance Awareness Program. The IAO shall ensure that the program meets or exceeds the IA training requirements set forth in DODI 8570.1.

### **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 IA requirements
- Develop training to satisfy the IA 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 IA applicable policies. Examples of ALMR policies that directly relate to IA include, but are not limited to:

- System Recovery Policy 400-1
- System Incident Response Policy 400-2
- System Account Control Policy 400-4

2.6.2 All System users 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 IA 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, consultant, temporary employee, or other personnel that utilize 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 IA Awareness orientation training. This training shall be a condition of access to, or use of, the ALMR System and can be provided in classroom, computer-based, or blended formats under the guidance of the ALMR IA0.

3.1.3 By the end of IA 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 IA 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 point(s) 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, test, and troubleshoot IA-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 IAO/Security Manager

3.3.3 Individuals identified as the ALMR IAO/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 DODI 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 user agency POC shall contact the ALMR Help Desk and initiate a New User Access Request.

## **4.2 Yearly Training Review**

All Level II and Level III System users are required to renew their training certificate yearly in an effort to ensure the appropriate level of IA 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 IA Awareness Orientation training should include, at a minimum, the following topics as they apply to the ALMR System:

- What IA 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 IA Orientation Training
- Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) 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 IA-related repairs
- Lead teams to quickly solve IA-related issues
- Determine if a security incident is a violation of ALMR policy, or relevant laws
- Monitor and evaluate the effectiveness of the IA 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

#### **5.4 Training Records**

The IAO/Security Manager shall maintain training records for all System users, which note each individual user's employment agency and training level status. The IAO/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 Information Assurance Awareness Procedure is outlined in ALMR Information Assurance Awareness Policy Memorandum 200-5.

## Reference Documents

1. DODI 8500.2, Information Assurance Implementation,  
<http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>
2. NIST SP800-53, Recommended Security Controls for Federal Information Systems,  
<http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf>
3. Department of Defense Information Assurance Workforce Improvement Program  
8570.01-M, <http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>
4. Department of Defense Instruction 8570.1 “Information Assurance Training,  
Certification, and Workforce Management,”  
<http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf>