



Alaska Land Mobile Radio Communications System

Privileged User Acceptable Use Procedure 400-7

Version 3

April 5, 2011

Developed in conjunction 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 Privileged Users | 1 |
| 3.0 Acceptable Use | 5 |
| 3.1 Data Classification | 5 |
| 3.2 Public Key Infrastructure Use | 5 |
| 4.0 Compliance | 5 |
| Attachment 1 Privileged User Acknowledgement and Consent Form | 6 |



Document Revision History

| Name | Date | Reason for Changes | Version |
|----------------|-------------|-------------------------------------------------------------|----------------|
| Huls, Chad | 2/2/2009 | Approved by the User Council – Final. | 1 |
| Shafer, Sherry | 3/5/2010 | Annual review. Approved by the User Council – Final. | 2 |
| Shafer, Sherry | 4/05/2011 | Annual review/update. Approved by the User Council - final. | 3 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |



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 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.

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).



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 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 Manager: the Operations Manager represents the User Council interests and makes decisions on issues related to the day-to-day operation of the system and any urgent or emergency system operational or repair decisions. In coordination with the User Council, the Operations Manager establishes policies, procedures, contracts, organizations, and agreements that provide the service levels as defined in the ALMR Service Level Agreement.

Privileged User/Member: any agency, person, group, organization or other entity which has an existing written Membership Agreement to maintain or operate on ALMR with one of the Parties to the Cooperative Agreement is a privileged user. The terms privileged user and member are synonymous and interchangeable.

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

This procedure defines terms and conditions for all users operating on the Alaska Land Mobile Radio (ALMR) Communications System according to the classification level of information to which they have been granted access. Access levels for ALMR are set forth by the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) and in accordance with Department of Defense (DOD) Directive 8500.1, Information Assurance (IA), October 24, 2002, and DOD Instruction 8500.2, Information Assurance (IA) Implementation, February 6, 2003.

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 Privileged User Acceptable Use Policy & Procedure warrant such action.

2.2 User Council

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

2.3 System Management Office

The System Management Office (SMO) shall inform the Information Assurance Officer (IAO)/Security Manager and the Operations Manager of any suspect activities, System information compromises, training discrepancies, etc.

2.4 Security Manager

2.4.1 The IAO/Security Manager shall:

- Ensure each privileged system user acknowledges understanding of this procedure through a signed copy of the ALMR Privileged User Acknowledgement and Consent Form (Appendix A)
- Make recommendations to the Operations Manager, User Council, and Executive Council concerning sanctions against any user who violates these procedures

2.5 Privileged Users

Any agency, person, group, organization or other entity which has an existing written Membership Agreement to maintain or operate on ALMR with one of the Parties to the Cooperative Agreement is a privileged user. All ALMR privileged users have the



responsibility to safeguard against unauthorized or inadvertent modification, disclosure, destruction, denial of service, and misuse of privileges as defined in the following categories:

- **Access Terminal Operators** – this group of individuals are responsibility for ALMR systems setup, maintenance and monitoring activities. This group includes the OMO, SMO, other contractor and user organizations staff assigned these responsibilities. This user group poses the highest risk to the ALMR System because of their user privileges, requires the highest level of technical training and annual refresher training to insure the system is not compromised.

Each user in the group shall:

- Configure and operate IA and IA-enabled technology according to DOD Information Systems (IS) IA policies and procedures and notify the IAO/Security Manager of any changes that might have an adverse impact on the System
- Establish and manage authorized user accounts for the ALMR System, including configuring access controls to enable access to authorized information, and removing authorizations when access is no longer needed
- Ensure users possess the appropriate background investigation commensurate with level of access granted and, where appropriate, have a signed non-disclosure agreement on file with the ALMR IAO/Security Manager
- Complete Annual IA Awareness Training Level III and provide proof of completion to the SMO and their immediate supervisor
- Generate and protect passwords or pass-phrases (passwords should not be written down, but instead committed to memory, unless recording them is required by operational circumstances and the record document is secured)
- Use only authorized hardware and software on the ALMR System(The user will not install or use any personally owned hardware, software, shareware, or public domain software)
- Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized
- Not alter, change, configure, or use operating systems, programs, or information systems except as specifically authorized by the SMO
- Safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the ALMR information systems
- Not disseminate ALMR System information to anyone without a specific need to know as verified by the Security Manager or assigned agent
- Not utilize DOD-provided information systems for commercial or financial gain, including, but not limited to, illegal activities
- Be subject to all US criminal, civil, and administrative laws regulating appropriate use of government information systems



- Immediately report any suspicious output, files, shortcuts, or System problems to the SMO, Security Manager, and/or the IAO
 - Inform the IAO/System Manager when access to the ALMR System is no longer required (e.g. completion of project, transfer, retirement, resignation)
 - Not unilaterally bypass, strain, or test IA mechanisms. If IA mechanisms must be bypassed, users shall coordinate the procedure and receive written approval from the IAO/Security Manager
 - Address any questions regarding policy, responsibilities, and duties to the IAO/Security Manager
 - Understand that violation of this, or any security measure, could result in the loss of access privileges
- **Console Terminal Operators** – this group of individuals are responsible for staffing Emergency Operation Center, Command Center and Dispatch Center operations. This user group poses the second highest risk to the ALMR System because of their user privileges, requires a high level of training and annual refresher training to insure the system is not compromised.

Each user in this group shall:

- Establish and manage authorized user accounts for the ALMR System, including configuring access controls to enable access to authorized information, and removing authorizations when access is no longer needed
- Ensure users possess the appropriate background investigation commensurate with level of access granted and, where appropriate, have a signed non-disclosure agreement on file with the ALMR IAO/Security Manager
- Complete Annual IA Awareness Training Level II and provide proof of completion to the SMO and their immediate supervisor
- Generate and protect passwords or pass-phrases (passwords should not be written down, but instead committed to memory, unless recording them is required by operational circumstances)
- Use only authorized hardware and software on the ALMR System(The user will not install or use any personally owned hardware, software, shareware, or public domain software)
- Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized
- Not alter, change, configure, or use operating systems, programs, or information systems except as specifically authorized by the SMO
- Safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the ALMR information systems
- Not disseminate ALMR System information to anyone without a specific need to know as verified by the Security Manager or assigned agent



- Not utilize DOD-provided information systems for commercial or financial gain, including, but not limited to, illegal activities
 - Be subject to all US criminal, civil, and administrative laws regulating appropriate use of government information systems
 - Immediately report any suspicious output, files, shortcuts, or System problems to the SMO, Security Manager, and/or the IAO
 - Inform the IAO/System Manager when access to the ALMR System is no longer required (e.g. completion of project, transfer, retirement, resignation)
 - Not unilaterally bypass, strain, or test IA mechanisms. If IA mechanisms must be bypassed, users shall coordinate the procedure and receive written approval from the IAO/Security Manager
 - Address any questions regarding policy, responsibilities, and duties to the IAO/Security Manager
 - Understand that violation of this, or any security measure, could result in the loss of access privileges
- **Subscriber Radio Users** – this group of individuals comprises the majority of ALMR users. Although they pose less risk to the ALMR System than Access Terminal Operators and Console Terminal Operators they can still compromise the system by allowing unauthorized or inappropriate use of a subscriber radio. This user group requires training and annual refresher training to insure the system is not compromised.

Each user shall:

- Establish and manage authorized user accounts for the ALMR System, including access to authorized information, and removing authorizations when access is no longer needed
- Ensure users possess the appropriate background investigation commensurate with level of access granted and, where appropriate, have a signed non-disclosure agreement on file with the ALMR IAO/Security Manager
- Use only authorized hardware and software on the ALMR System(The user will not install or use any personally owned hardware, software, shareware, or public domain software)
- Complete Annual Subscriber Radio Training Level I which includes IA Training and provide proof of completion to the OMO/SMO and their immediate supervisor
- Safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the ALMR information systems
- Not disseminate ALMR System information to anyone without a specific need to know as verified by the Security Manager or assigned agent
- Not utilize DOD-provided information systems for commercial or financial gain, including, but not limited to, illegal activities



- Be subject to all US criminal, civil, and administrative laws regulating appropriate use of government information systems
- Inform the IAO/System Manager when access to the ALMR System is no longer required (e.g. completion of project, transfer, retirement, resignation)
- Not unilaterally bypass, strain, or test IA mechanisms. If IA mechanisms must be bypassed, users shall coordinate the procedure and receive written approval from the IAO/Security Manager
- Address any questions regarding policy, responsibilities, and duties to the IAO/Security Manager
- Understand that violation of this, or any security measure, could result in the loss of access privileges

3.0 Acceptable Use

All ALMR users must understand they have the primary responsibility to safeguard ALMR information. They also have the responsibility to protect the System from, and report any unauthorized or inadvertent modification, disclosure, destruction, denial of service, and misuse. Access to any ALMR resource is a revocable privilege and is subject to constant monitoring and security testing.

3.1 Data Classification

All data on the ALMR System is deemed “For Official Use Only,” and as set forth in Federal and DOD directives. The highest level of classification for voice and data traffic on the System is “Sensitive But Unclassified.”

3.2 Public Key Infrastructure Use

3.2.1 For the purposes of acceptable use for encrypted communications conducted on the ALMR System, Public Key Infrastructure (PKI) provides a secure computing environment utilizing asymmetric encryption (public/private-keys) and is used to encrypt information and verify the origin of the receiver

3.2.2 Any access to PKI systems, encryption keys, and other resources in relation to the PKI used on the ALMR System is privileged and is granted on an as-needed basis. ALMR users agree to ensure all PKI-related information and systems are safeguarded, and that no information is disclosed or access given to an unauthorized individual.

4.0 Compliance

Compliance with the Privileged User Acceptable Use Procedure is mandatory and is outlined in ALMR Privileged User Acceptable Use Policy Memorandum 400-7.



Attachment 1 Privileged User Acknowledgement and Consent Form

I, _____, have read the ALMR Privileged
(Print Full Name)

User Acceptable Use Procedure 400-7, and accept the terms and conditions set forth in the policy document. I give the ALMR Executive Council the right to use my personal information for the purpose of complying with US Federal Directives allowing me access to the ALMR network environment. I understand that if I violate the rules of this policy my access can be terminated and I may face disciplinary measures including administrative sanction or criminal prosecution.

Name (Printed)

Signature

Date

ALMR Security Manager or IAO Signature