Alaska Land Mobile Radio Communications System

System Recovery Procedure 400-1

Version 11

August 18, 2017

Developed in conjunction 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 Operations Management Office 1
2.4 System Management Office 1
2.5 Security Manager 2
3.0 Disaster Response Process **3**
3.1 Stages 3
3.2 Off-Site Recovery 3
3.3 Hard Disk Failure 3
3.4 Device Failure 4
3.5 Power Failure 4
3.6 Accidental Deletion or Modification of Critical Data 4
3.7 Theft or Sabotage 4
3.8 Virus Attack 4
3.9 Network Failure 4
3.10 Software Failure 5
4.0 Prioritization of Recovery **5**
5.0 Secure Recovery **5**
6.0 Training and Awareness **5**
7.0 System Recovery Plan Testing **6**
8.0 Compliance **6**

Document Revision History

Name	Date	Reason for Changes	Version
Shafer, Sherry	3/20/2008	Approved by the User Council – Final.	2
Shafer, Sherry	3/23/2009	Annual Review; approved by the User Council – Final.	3
Shafer, Sherry	3/17/2010	Annual review. Approved by the User Council – Final.	4
Shafer, Sherry	4/05/2011	Annual review/update. Approved by the User Council - final.	5
Shafer, Sherry	7/26/2012	Annual review/update. Approved by the User Council - final.	6
Shafer, Sherry	7/30/2013	Annual review/update. Approved by the User Council - final.	7
Shafer, Sherry	7/29/2014	Annual review/update. Approved by the Operations Management Office – final.	8
Shafer, Sherry	8/3/2015	Annual review/update. Approved by the Operations Management Office – final.	9
Shafer, Sherry	8/22/2016	Annual review/update. Approved by the Operations Management Office – final.	10
Shafer, Sherry	8/18/2017	Annual review/update. Approved by the Operations Management Office – final.	11

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: Cybersecurity replaces and is synonymous with Information Assurance (IA) IAW Department of Defense Instruction (DoDI) 8500.01, *Cybersecurity.* Cybersecurity is the 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).

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.

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.

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 Council (UC): 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 provides the basis for the appropriate management and security of the Alaska Land Mobile Radio (ALMR) Communications System. A well-protected network enables organizations to easily handle the increasing dependence on voice and data communication systems in the event of an emergency.

This procedure provides information on the roles of personnel assigned to, or utilizing, the System. It also outlines the organizational resources and controls in place for recovery of the ALMR System in the event of a disaster and meets the requirements of the DOD Instruction (DODI) 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*.

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 System Recovery Procedure warrant such action.

2.2 User Council

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

2.3 Operations Management Office

The Operations Management Office (OMO) will brief the EC and the UC in the event of a System disaster requiring recovery operations. The OMO will also prepare the associated Situation Reports (SITREPs), as outlined in ALMR Emergency Operations Procedure 300-5.

2.4 System Management Office

The System Management Office (SMO) shall:

- Maintain 24-hour contact information for key maintenance personnel and key vendors
- Maintain information required to access or obtain spare technology assets
- Coordinate with the Security Manager in the event that System maintenance or spare equipment is required to properly implement a System Recovery Plan
- Ensure that the appropriate personnel from the contact list are convened as members of the ALMR System Recovery Team and establish a central meeting location. The team shall include lead members from each major area of the ALMR System and necessary resources for recovery efforts

- Coordinate the System recovery and ensure that the recovery is performed by the appropriate technical teams

2.5 Security Manager

The Security Manager (SCM) shall:

- Assign security priorities and approve security standards based on a system with a security impact of moderate confidentiality, high integrity, and high availability
- Develop, disseminate and periodically review/update the formal, documented System Recovery Procedure that addresses purpose, goals, and roles and responsibilities
- Work in conjunction with the System Manager to create, implement and manage an ALMR System Recovery Plan and oversee actions taken by responsible parties ensuring that such actions do not negatively impact the integrity or availability of the ALMR System
- Designate an individual to be responsible for providing security-related information to ALMR management for potential release to media and public entities regarding any System event in accordance with ALMR Records Management Procedure 300-1
- Designate an individual to be responsible for coordinating efforts with outside response resources to ensure recovery efforts abide by required laws and agreements
- Review System Recovery Plan test results to identify issues within the training curriculum
- Address and manage identified issues under the scope of System Recovery and report violations to the EC, through the OMO. Any suggested action to be taken in the form of a sanction shall be documented by the Security Manager and must be approved by the EC

2.6 System Users

All System users should be able to recognize a potential security violation and then take appropriate action to report the incident.

Those users with higher levels of responsibility possess specialized technical experience and are in a position to identify system intrusions and system vulnerabilities (see Cybersecurity Procedure 200-5). Individuals utilizing ALMR should report any suspicious activity to the SMO or SCM, as soon as it is detected.

3.0 Disaster Response Process

The System Recovery Team shall develop a System Recovery Plan based on the type and scope of the disaster. The plan shall enable partial resumption of mission- or business-essential functions within five days of activation.

If it is determined by the SCM that it is not possible to obtain partial resumption of mission- or business-essential functions at the primary site within this time period, then the off-site recovery location will be used for resumption.

3.1 Stages

The System Recovery Plan consists of the following stages:

- Detect disaster condition
- SMO contacts key personnel and convenes a System Recovery Team
- System Recovery Team creates a System Recovery Plan appropriate to the type and scope of the disaster
- SMO invokes System Recovery Plan
- Security Manager provides information to ALMR management for potential release to the public
- System restoration
- Return to normal operation

NOTE: The System Recovery Plan, created in the event of a disaster, shall use current industry standard practices, whenever possible, and shall take advantage of any existing business recovery plans, system contingency plans, facility recovery plans, etc.

3.2 Off-Site Recovery

The System Recovery Plan shall identify and specify arrangements for an alternate site that permits the partial restoration of mission- or business-essential functions, when applicable.

In the event of significant or total destruction of a Master Site of the ALMR System, the alternative recovery location shall be the Master Site of one of the other zones, which can be reprogrammed to provide full restoration of the System.

3.3 Hard Disk Failure

Backup hard disks will be available to replace a failed hard disk in any System component. The SMO will coordinate the replacement of parts and services. After replacement, System data will be restored to the new disk using the most current backup.

3.4 Device Failure

Server failure can be the result of a failure of any component of the server including: CPU, memory, PCI adapters, LAN controllers, power, etc. Backup server components will be available to replace a failed server component. The SMO will coordinate the replacement of parts and services.

3.5 Power Failure

Power failure can be the result of dangerously high voltages, power shortage or complete power failure. The ALMR System will be equipped with surge protection devices to protect against a fluctuation in power. An alternative power source for ALMR sites shall be available in the event that power is completely lost. The SMO will coordinate the use of the alternate power source in the event of a power failure.

3.6 Accidental Deletion or Modification of Critical Data

In the event of accidental deletion or modification of critical data, the System Recovery Team shall take advantage of the most current backup data for restoral of the ALMR System.

3.7 Theft or Sabotage

The SMO/SCM will respond to theft or sabotage by first categorizing the damage as either damage to physical components or damage to information. In the event of physical damage, the System Response Team will respond as indicated in Section 3.3 or 3.4. If the damage is to information, software or data, the SMO will respond as indicated in Section 3.6 or 3.8.

3.8 Virus Attack

The SCM will respond to a virus attack as indicated in the ALMR Incident Response Procedure 400-2. In the event that a system cannot be returned to working conditions within an acceptable period of time as determined by the SCM, the affected device will be replaced with a functioning backup device.

3.9 Network Failure

Network failure can be caused by a variety of issues. In the event of network failure, the SMO will identify the reason for the failure and respond with the appropriate action, based on the cause of the failure.

If the failure is caused by a device failure, the SMO will coordinate the replacement of the part(s) and services. If the network failure is due to a virus attack, human

interaction (intentional or otherwise), or malicious software, etc., the SCM will respond as dictated by ALMR System Incident Response Policy 400-2.

3.10 Software Failure

The SMO will respond to a software failure on any ALMR system by first troubleshooting the software error. If the System cannot be returned to working condition within an acceptable period of time, it will be reverted to the last known good configuration, reinstalled, or restored from the current backup.

4.0 Prioritization of Recovery

In the event of a disaster, a System Recovery Plan shall identify mission- and business-essential functions. The identified functions shall have an assigned priority for restoration as outlined in ALMR System Backup and Recovery Procedure 400-5, Attachment 1.

5.0 Secure Recovery

Recovery procedures, and required System functionality, shall be specified within the System Recovery Plan to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery shall be documented and appropriate mitigating procedures will be designated.

If appropriately cleared personnel, as defined by the SCM, 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 outlined in ALMR System Backup and Recovery Procedure 400-5.

Any component, which is determined to no longer be in an acceptable functioning state, must be decommissioned in a secure manner. Once an ALMR System computing asset is targeted to be replaced or discarded as a result of defect, each asset must be properly cleared and sanitized, or destroyed (see Information Systems Clearing and Sanitization Procedure 200-4). These actions must be documented in the form of a report and results provided to the Asset Manager for retention.

6.0 Training and Awareness

To successfully comply with Cybersecurity requirements under the Department of Defense Risk Management Framework (RMF) for DoD Information Technology (IT), System recovery planning should be an integrated part of the user culture. A lack of established controls for System recovery exposes the ALMR System to risks including attacks, compromise of network systems and services, legal issues and potential Denial of Authority to Operate (DATO).

All personnel who possess an ALMR System user account shall receive annual Cybersecurity training that defines their potential disaster recovery responsibilities.

7.0 System Recovery Plan Testing

The System Recovery Plan shall be tested annually and all results of the test shall be recorded. The SCM shall be responsible for overseeing the testing and verifying that the results have been recorded. Results of the testing will be presented to the UC. **NOTE**: The results of the System Recovery Plan test shall be combined into a single report with the results of the annual Backup and Recovery test (see System Backup and Recovery Procedure 400-5) as both reports cover much of the same information. The report shall be produced and presented to the OMO at the end of the calendar year.

The SCM shall be responsible for updating the System Recovery Procedure based on the results of the annual testing, as necessary.

8.0 Compliance

Compliance with the System Recovery Procedure is outlined in ALMR System Recovery Policy Memorandum 400-1.