Alaska Land Mobile Radio Communications System

Emergency Operations Procedure 300-5

Version 10

April 16, 2018

Table of Contents

Document Revision History

Name	Date	Reason for Changes	Version
Shafer, Sherry	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	12/23/2011	Annual review/update. Approved by the User Council – final.	3
Shafer, Sherry	4/20/2012	Annual review/update. Approved by the User Council - final.	4
Shafer, Sherry	4/2/2013	Annual review. Approved by the Operations Management Office - final.	5
Shafer, Sherry	4/22/2014	Annual review/update. Approved by the Operations Management Office - final.	6
Shafer, Sherry	4/20/2015	Annual review/update. Approved by the Operations Management Office - final.	7
Shafer, Sherry	4/19/2016	Annual review. Approved by the Operations Management Office - final.	8
Shafer, Sherry	4/11/2017	Annual review. Approved by the Operations Management Office - final	9
Shafer, Sherry	4/16/2018	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 and Mutual Aid Agreement.

Alaska Municipal League: a voluntary non-profit organization in Alaska that represents member local governments.

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).

For Official Use Only (FOUO): this designation is used within the Department of Defense and the Department of Homeland Security to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact the conduct of federal programs, or other programs or operations essential to the national interest.

Freedom of Information Act (FOIA): a law ensuring public access to U.S. government records. FOIA carries a presumption of disclosure; the burden is on the government - not the public - to substantiate why information may not be released. Upon written request, agencies of the United States government are required to disclose those records, unless they can be lawfully withheld from disclosure under one of nine specific exemptions in the FOIA. This right of access is ultimately enforceable in federal court.

Information Assurance (IA)/Cybersecurity: 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.

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.

Minimize: essential, concise and to-the-point radio traffic only.

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 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.

Operations Management Office (OMO): develops recommendations for policy, 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.

Security Categorization: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

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 states' microwave system), and shared owner of 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.

User Council (UC): 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 serves as the guideline for defining the roles and responsibilities of the Operations Management Office (OMO) and System Management Office (SMO) in the performance of mission-essential services for the restoration of the Alaska Land Mobile Radio (ALMR) Communications System during emergency response to manmade or natural disaster crises.

2.0 Roles and Responsibilities

2.1 Executive Council

The Executive Council (EC) shall be responsible for:

- Management and enforcement of sanctions when violations of the Emergency Operations Procedure warrant such action
- Monitoring communications and situational reports provided by the Operations Manager/System Manager and providing direction, as needed

2.2 User Council

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

2.3 Operations Management Office

The OMO shall be responsible for:

- Responding accordingly in the case of a disaster, manmade or natural
- Coordinating with the System Manager to assess System status and bring the System fully back on line, as soon as possible
- Keeping the EC and the UC informed of any changes in System status, to the greatest extent possible
- Overseeing the generation of required reports and notifications outlined in this procedure

2.4 System Management Office

2.4.1 The SMO shall be responsible for:

- Maintaining contact lists, process flows, lists of subject matter experts and configuration procedures for the System
- Ensuring System backups are kept up to date, as outlined in ALMR System Backup and Recovery Procedure 400-5

- Requiring all vendors and user agencies participating on the System, in any way, to provide incident response points of contact and an internal means to initiate immediate contact

2.5 Security Manager

The Security Manager (SCM) shall be responsible for:

- Ensuring appropriate operational security posture is maintained for the System, in the event of a disaster
- Determining the existence and severity of any System security compromise
- Responding in accordance with applicable security procedures
- Reporting critical security concerns to the OMO and the Functional Commander (FC)/Authorizing Official (AO)

2.6 System Administrators and Technicians

System administrators and technicians will take direction from the SMO/SCM, as necessary.

3.0 Initial Incident Response

When a catastrophic event happens, the closest OMO/SMO staff member (pre-designated) will respond to the Tudor Road Master Site, as soon as safely possible. At a minimum, the Operations Manager, System Manager and a System Technologist will respond to all catastrophic events. Other required individuals will proceed, as soon as permitted by the nature of the disaster.

If unable to reach the Tudor Road Master Site due to loss or damage to transportation infrastructure, the required staff shall make every attempt to contact the Tudor Road Master Site via remote log in from an ALMR site, land line, cell phone or subscriber unit.

If the Tudor Road controller is not accessible, the System Manager shall contact the North Zone System Technologist, who shall proceed to the Birch Hill controller, evaluate the status of the ALMR System and report back to the System Manager. The System Manager will confer with the Operations Manager, at such time.

In the case of a major emergency spanning up to a four-day weekend (extended holiday weekend), the OMO may be required to staff the office on a 24-hour basis. Emergency operation requirements are determined by the OMO and SMO, after consultation with the ALCOM/J6 and the State of Alaska (SOA) Office of Information Technology (OIT).

3.1 System Assessment

3.1.1 Upon arrival, the first available staff member will access the Network Management Terminal and do an initial assessment of available sites using Site Status Reporting Procedures (Appendix A).

3.1.2 The staff member shall contact the Operations Manager/System Manager and provide a briefing on the current System status, as soon as possible.

The initial assessment shall determine the level of response necessary beyond the minimum required personnel.

3.1.3 The OMO, SMO and SCM, in coordination with OIT and other participating agencies/individuals, as dictated by the severity of the disaster, shall make a determination as to the priority order in which to bring affected geographic areas back on line.

Additionally, all non-essential System traffic may be restricted (minimized) if System busies exceed the emergency operations acceptable busy level, as determined by the System Manager. Agencies will be notified, to the greatest extent possible, when minimize is in effect.

3.2 Incident Notification

Once the System status is assessed, the Operations Manager will contact the EC members (as available) to provide an initial Situation Report (SITREP) and receive any further direction.

Following receipt of direction, the Operations Manager will notify the ALCOM/J6, (unless already notified as an EC member) or his/her designated representative and the SOA OIT SATS/ALMR Manager, or his/her designated representative.

3.3 Reporting

The following sections describe the reports required for incident response efforts.

NOTE: All reports will utilize the current Zulu time.

3.3.1 Communications Spot Report (COMSPOT)

COMSPOTs are due within ten minutes of an outage or event, or as soon as practical. COMSPOTs will be updated, as needed, when the status changes or updated information is available. A final COMSPOT is due when full operational service is restored.

Template:

- Report Type (Initial, Update, Final)
- Start Time (DDHHMMZ MMM YY)(meaning two-digit day, two-digit hour, two-digit minute, Z for Zulu time, a space, three-character month, a space and two-digit year)
- Stop Time (DDHHMMZ MMM YY)
- Unit or Organization and Location Affected
- Event
- Network(s) or Service(s) Affected
- O&M Unit or Organization
- Estimated Time to Return to Operation (ETRO)/Point of Contact (POC)
- Fix Action
- Mission Status
- Current Status

3.3.2 Situation Report (SITREP)

3.3.2.1 SITREPs should include a list of all affected sites with verbiage to indicate status.

GREEN = fully operational,
YELLOW = degraded (COMSPOT should be sent)
RED = no capability (COMSPOT should be sent)

NOTE: Any site reported as YELLOW or RED will require additional explanation of status of the site, current maintenance activities, unit(s)/organization(s) impacted (with the impact explained) and ETRO.

3.3.2.2 Content.

SITREPs will contain:

- Time and nature of the incident
- Impact of the incident on System assets and current status
- Temporary actions taken to mitigate/minimize loss or impact on System assets
- Designated ICS Zones activated
- Estimated timeframe for System restoral, if applicable and feasible
- Personnel contacted/on duty

3.3.2.3 Distribution and timeline.

SITREPs will be distributed to the following personnel/agencies, as communications mediums are available (at a minimum):

- EC
- UC

- State Emergency Coordination Center (SECC)
- Anchorage, Fairbanks, Mat-Su and Soldotna Emergency Operations Centers (EOCs)

SITREPs will be generated on the following schedule:

- Upon initial System assessment
- Hourly, after the initial SITREP, for the first 24 hours
- At shift change until the emergency is declared ended

3.3.3 Situation Normal (SITNORM)/All Clear Report

A SITNORM Report shall be completed by the OMO/SMO at the conclusion of all response efforts.

3.3.3.1 Content.

SITNORMs will describe:

- An executive summary of the disaster
- The timeline of the disaster
- The nature of the disaster
- The operational impact of the disaster
- How the incident was identified
- Action(s) taken to restore the System to its pre-incident condition
- Loss of any System assets resulting from the disaster
- Short- and long-term impact and suggested mitigation efforts

3.3.3.2 Distribution and timeline.

SITNORMs will be distributed within two business days to (at a minimum):

- EC
- UC
- State ECC
- Anchorage, Fairbanks, Mat-Su and Soldotna EOCs

3.4 After-Action Review

An after-action review of the event shall be completed within 30 days of the conclusion of an event. This review will examine the effectiveness of the response and any areas requiring improvement. All participating members shall provide input during this process.

Areas to be considered during this review include:

- Incident response availability
- Initial incident assessment
- Recovery efforts

- Effectiveness of procedures
- Procedural gaps
- Complicating factors that affected the incident response effort

3.5 Record Retention

Records will be maintained in accordance with ALMR Records Management Policy and Procedure 300-1.

3.6 External Information Sharing

Any information pertaining to the disaster and its affects on the ALMR System, personnel, capabilities, readiness, physical location(s) or any privileged aspect of the System or its resources may not be disseminated without written permission of the EC.

The nature of a given disaster may require communication with one or more external organizations. This communication must be made in accordance with any additional reporting procedures, as defined by the Security Manager, and approved in writing by the EC.

3.7 Public Media Disclosure

The System is rated as a Moderate Confidentiality, Moderate Integrity and Moderate Availability system. In accordance with ALMR System Incident Response Procedure 400-2, information carried by and stored on the ALMR network does not exceed a classification of UNCLASSIFIED, but information on ALMR may be For Official Use Only (FOUO), Privacy Act or other sensitive type data. Disclosure of any security breach of the ALMR System is exempt from the Freedom of Information Act (FOIA).

3.7.1 Release approval. Approval by the SCM, the SOA OIT and the Alaskan Command J6 must be obtained before any information relative to the ALMR System is released to public media, as outlined in ALMR Records Management Procedure 300-1, paragraph 6.5, Release of Records.

3.7.2 Law Enforcement. In the event that law enforcement involvement is required to mitigate a System disaster, the Security Manager shall serve as the primary contact for law enforcement.

While disclosure of a security incident is not required to be made public under FOIA, if information has been submitted as evidence in a court proceeding, it may not be excluded from FOIA.

4.0 Compliance

Compliance with the Emergency Operations Procedure is outlined in ALMR Emergency Operations Policy Memorandum 300-5.

Appendix A
Site Status Reporting Procedures

1.0 Signing on to the Network Management Terminal (NMT)

The following steps are required to provide an ALMR operational site overview for use in daily and emergency status reports.

These procedures require OMO/SMO personnel have the appropriate access to the Motorola® PRNM Suite Software Application on an ALMR Network Management (NM) Client Computer. To obtain a login and password for the NM Client Computer and the Motorola® PRNM Suite contact the ALMR Security Manager.

To access the Zone Watch software, a component of the Motorola® PRNM Software Suite, perform the following steps:

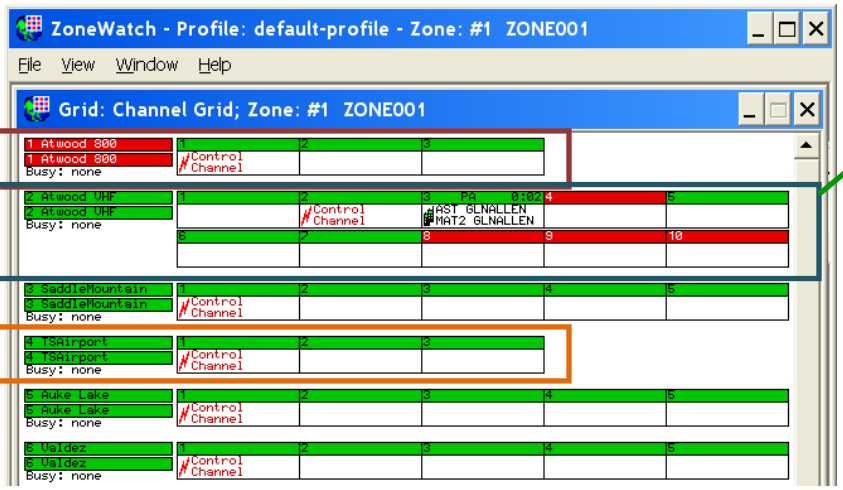
1. Power on and log into the SMO NM Client Computer
2. Locate the PRNM Suite Icon on the desktop and double-click on it to Launch.
3. Upon successful launch of the PRNM Suite, select "**Primary Zone Core** from the open explorer window
4. Select "**ZONE001**" or "**ZONE002**.
5. Select "**ZONE001 ZoneWatch**" or "**ZONE002 ZoneWatch**" and double-click on icon to launch.
6. Select "**Everything**" and press "**Open**". (repeat the process from step 4 to open the other Zone)
7. "This will open the ZoneWatch windows for Zone001 and Zone002. The Zone Watch application will display the status of each site and its channels.

2.0 Determining Wide Area Trunking and Site Channel Status

The following image and descriptions provide an example of how to interpret the ZoneWatch display and determine the status of each site and its channels.

When the Site Name is highlighted in red the site and all its channels status is "unknown".

When the Site Name as well as all the channels is highlighted in green the site is fully operational.
NOTE: Operational, but inactive, channels are highlighted in orange.



When the Site Name is highlighted in green but some or all of the channels are red, the site is currently in wide trunking, but the channels highlighted in red should be noted and reported as down or with a status of unknown.

The status of all sites in both Zone001 and Zone002 should be determined and entered into the site status sheets. Any sites and/or channels with an unknown status will be displayed in red and should be noted on emergency and daily reports.

The following site status sheets shall be utilized for each zone during the initial assessment of the System status in a disaster and should also be used to disseminate site status information.

2.1 Zone 1 Site Status Sheet

Site Name	Site Status (Wide Area Trunking, Site Trunking, Down, Unknown)	Additional Comments
Alcantra		
Anchor River		
Atwood		
Auke Lake		
Bailey Hill		
Blueberry Hill		
Byers Creek		
Chulitna		
Cooper Mountain		
Cottonwood Creek		
Diamond Ridge		
Dimond Courthouse		
Divide		
Ernestine Mountain		
Fire Station 12		
Girdwood		
Glennallen		
Goose Creek 700MHz		
Haines		
Heney Range		
High Mountain		
Honolulu		
Hope		
Hurricane		
Kasilof		
Kenai		
Lena Point		
Lions Head		
Moose Pass		
New Knik		
Nikiski		
Ninilchik		
Pillar Mountain		
Pipeline Hills		
Portage		
R1 North		
Rabbit Creek		
Saddle Mountain		
Sawmill		
Seldovia		

Site Name	Site Status (Wide Area Trunking, Site Trunking, Down, Unknown)	Additional Comments
Seward		
Silvertip		
Site Summit		
Sitka		
Skagway		
Ski Hill		
Sourdough		
Sterling		
Summit Lake		
Sunny Hay Mountain		
Tahneta Pass		
Ted Stevens Airport		
Tolsona		
Transportable Area South		
Tsina		
Tudor Road		
Valdez		
Whittier		
Willow Creek		
Willow Mountain		
Wolcott Mountain		
Womens Bay		

NOTE: St Paul Island does not have reach back capability to the rest of the System and is not included in this list.

2.2 Zone 2 Site Status Sheet

Site Name	Site Status (Wide Area Trunking, Site Trunking, Down, Unknown)	Additional Comments
Beaver Creek		
Birch Hill		
Black Rapids		
Canyon Creek		
Cathedral Rapids		
Clear AFS		
Delta		
Donnelly Dome		
Dot Lake		
Ester Dome		
Ft Greely		
Garner		
Harding Lake		
Hill 3265		
Independent Ridge		
Money Knob		
Nenana		
Paxson		
Peger Road		
Pole Hill		
Quarry Hill		
Reindeer Hills		
Transportable Area North		
Tok		
Trims		
Yanert		