



# **Alaska Land Mobile Radio Communications System**

## **Facility Security Penetration Procedure 200-2**

**Version V7**

April 10, 2017



## **Table of Contents**

<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 Overview .....</b>	<b>1</b>
<b>3.0 Roles and Responsibilities .....</b>	<b>1</b>
<b>3.1 Executive Council .....</b>	<b>1</b>
<b>3.2 User Council .....</b>	<b>1</b>
<b>3.3 Operations Management Office .....</b>	<b>1</b>
<b>3.4 System Management Office .....</b>	<b>2</b>
<b>3.5 Enterprise Technology Services Division .....</b>	<b>2</b>
<b>3.5 Trusted Agent/OMO Staff .....</b>	<b>2</b>
<b>4.0 After Action Review .....</b>	<b>2</b>
<b>5.0 Compliance .....</b>	<b>3</b>
<b>Appendix A Security Penetration Procedural Checklist .....</b>	<b>4</b>



## Document Revision History

<b>Name</b>	<b>Date</b>	<b>Reason for Changes</b>	<b>Version</b>
Shafer, Sherry	3/23/2011	Approved by the User Council - final.	1
Shafer, Sherry	4/20/2012	Annual review. Approved by the User Council - final.	2
Shafer Sherry	4/3/2013	Annual review. Approved by the Operations Management Office - final.	3
Shafer, Sherry	3/11/2014	Annual review/update. Approved by the User Council - final.	4
Shafer, Sherry	4/16/2015	Annual review/update. Approved by the User Council - final.	5
Shafer, Sherry	4/29/2016	Annual review. Approved by the Operations Management Office - final.	6
Shafer, Sherry	4/10/2017	Annual review. Approved by the Operations Management Office - final.	7



## **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 (AML):** a voluntary non-profit organization in Alaska that represents 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 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).

**Municipality of Anchorage (MOA):** the MOA covers 1,951 square miles with a population of approximately 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.

**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.



*Alaska Land Mobile Radio Communications System  
Facility Security Penetration Procedure 200-2*

**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:** the ALMR Communications System, as established in the Cooperative Agreement, and any and all System Design/System Analysis (SD/SA) and System Design/System Implementation (SD/SI) documents.

**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:** 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 under the direction and guidance of the Executive Council.



## **1.0 Purpose**

This document serves as the guideline for conducting annual testing of the physical security measures protecting the Alaska Land Mobile Radio (ALMR) Communications System at 5900 E Tudor Road and defines the roles and responsibilities for the Operations Management Office, System Management Office and the State of Alaska (SOA) Enterprise Technology Services (ETS) Division.

## **2.0 Overview**

The ALMR System has two primary zone controllers; one is located in the North Zone and one located in the South Zone. The Zone 2 (North Zone) controller is located away from the general public on Fort Wainwright where access to the installation is controlled by the Department of Defense. The Zone 1 (South Zone) controller is located at 5900 E. Tudor Road in the ETS building. Access to the general public is controlled by SOA ETS.

## **3.0 Roles and Responsibilities**

### **3.1 Executive Council**

The Executive Council (EC) shall be responsible for the management and enforcement of sanctions when violations of the Facility Security Penetration Procedure warrant such action.

### **3.2 User Council**

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

### **3.3 Operations Management Office**

The Operations Management Office (OMO) will:

- Ensure unannounced building security penetration testing is conducted once each calendar year, at a minimum
- Prepare an audit report of findings and provide a copy to SOA ETS
- Maintain a copy of the report on file
- Work with the SMO and ETS to update procedures and brief personnel, if unauthorized access is gained
- Brief the User Council on the results annually
- Challenge all unknown personnel without a valid access badge or any unescorted visitor



### **3.4 System Management Office**

The System Management Office (SMO) will:

- Challenge all unknown personnel without a valid access badge or any unescorted visitor
- Ensure the zone controller room is properly secured at all times
- Ensure ALMR personnel are aware and trained on access requirements and procedures

### **3.5 Enterprise Technology Services Division**

The Enterprise Technology Services (ETS) Division will:

- Challenge all unknown personnel without a valid access badge or any unescorted visitor
- Ensure the zone controller room is properly secured at all times
- Ensure ETS personnel are aware and trained on access requirements and procedures

### **3.5 Trusted Agent/OMO Staff**

Under direction of the Operations Manager, any/all of the following shall be attempted by a trusted agent/staff member

- Attempt to gain access directly through the reception desk entry point, fail to obtain a visitor badge and/or fail to sign in
- Walk the perimeter and attempt to gain access through any unsecured door
- Attempt to roam the building unescorted and unchallenged
- Attempt to enter the Operations Management and System Management Offices and the zone controller area unchallenged, if building access is gained
- Attempt to leave the facility without signing out or returning the visitor badge
- Complete the security penetration checklist (Appendix A) to document the results

## **4.0 After Action Review**

Results of the facility penetration attempt, if successful, will be provided to SOA ETS by the Operations Manager. Procedural changes, if needed, will be discussed, agreed upon and implemented by each organization.

Both ALMR and ETS staff personnel will then be briefed, accordingly.



## **5.0 Compliance**

Compliance with the Facility Security Penetration Procedure is outlined in ALMR Facility Security Penetration Policy Memorandum 200-2.





## Appendix A Security Penetration Procedural Checklist

Yes	No	N/A	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unannounced visitor enters facility without checking in at the reception desk.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unannounced visitor is stopped upon entering the facility by the receptionist.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Receptionist inquires who the visitor is there to see.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Receptionist ensures that visitor signs in on the visitor log and is assigned and wears a visitor badge.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Receptionist calls person being visited and requests that they come and escort the visitor to their area, or escorts the visitor to the requested person/area.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Person being visited is not in. Alternative group/person (OMO or SMO) contact is attempted.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No internal contact can be made. Visitor is turned away.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Visitor requests access to the zone controller room. Was access granted by the SMO or ETS staff?
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unescorted visitor wanders around the facility and is stopped and questioned as to his/her business.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unescorted visitor gains access to the zone controller room, OMO or SMO office areas (circle each one that was penetrated).
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unescorted visitor leaves the facility without signing out and retains his/her visitor badge.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	OMO staff member/trusted agent walks the building perimeter and gains access through any unsecured door

**NOTE:** "N/A" means not applicable.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_