



*Alaska Land Mobile Radio Communications System  
Security Controls Review Procedure 200-6*



# **Alaska Land Mobile Radio Communications System**

## **Security Controls Review Procedure 200-6**

**Version 16**

December 3, 2025



*Alaska Land Mobile Radio Communications System  
Security Controls Review Procedure 200-6*

## **Table of Contents**

<b>Document Revision History .....</b>	<b>iii</b>
<b>Acronyms and Definitions .....</b>	<b>iv</b>
<b>1.0 Purpose .....</b>	<b>10</b>
<b>2.0 References .....</b>	<b>10</b>
<b>3.0 Roles and Responsibilities .....</b>	<b>10</b>
3.1 Executive Council .....	10
3.2 User Council .....	10
3.3 Information Systems Security Manager .....	10
<b>4.0 Security Controls Review Planning .....</b>	<b>11</b>
4.1 Review Objectives and Requirements .....	11
4.2 Information and Resources Under Review .....	11
<b>5.0 Assumptions .....</b>	<b>12</b>
<b>6.0 Approach to Security Controls Review .....</b>	<b>12</b>
6.1 Execution of Security Controls Review .....	13
6.2 Document Review Results .....	13
<b>7.0 Compliance .....</b>	<b>14</b>



*Alaska Land Mobile Radio Communications System  
Security Controls Review Procedure 200-6*

## Document Revision History

<b>Date</b>	<b>Reason for Changes</b>	<b>Version</b>
4/20/2009	Approved by the User Council – Final.	1
4/30/2010	Annual review/update. Approved by the User Council - Final.	2
5/9/2011	Annual review/update. Approved by the User Council - final.	3
8/24/2012	Annual review/update. Approved by the User Council - final.	4
9/3/2013	Annual review/update; approved by the Operations Management Office - final.	5
9/18/2014	Annual review/update; approved by the Operations Management Office - final.	6
9/8/2015	Annual review/update. Approved by the Operations Management Office - final.	7
12/13/2016	Annual review/update. Approved by the User Council – final.	8
12/27/2017	Annual review/update. Approved by the Operations Management Office - final.	9
12/19/2018	Annual review/update. Approved by the Operations Management Office - final.	10
12/21/2020	Annual review/update. Approved by the Operations Management Office - final.	11
12/8/2021	Annual review/update. Approved by the Operations Management Office - final.	12
12/1/2022	Annual review/update. Approved by the Operations Management Office - final.	13
12/13/2023	Annual review/update. Approved by the Operations Management Office - final.	14
12/11/2024	Annual review/update. Approved by the Operations Management, System Management, and Security Manager Offices - final.	15
12/3/2025	Annual review/update. Approved by the Operations Management, System Management, and Security Manager Offices - final.	16



## **Acronyms and Definitions**

**Agreement:** shortened term used to refer to the Cooperative and Mutual Aid Agreement, Service Level Agreement, or Membership Agreement within each associated document after the initial use.

**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, as established in the Cooperative Agreement and Mutual Aid Agreement.

**Alaska Municipal League:** a voluntary non-profit organization in Alaska that represents 165 cities, boroughs, and unified municipalities.

**Alaska Public Safety Communication Services (APSCS):** a State of Alaska (SOA) office in the Department of Public Safety (DPS) that operates and maintains the SOA Telecommunications System (SATS) supporting ALMR and providing public safety communication services and support to state agencies.

**ADP:** Automated Data Processing

**AES:** Advanced Encryption Standard

**AIS:** Automated Information System(s)

**C3I:** Command, Control, Communications, and Intelligence

**CAC:** Common Approval Chain

**Change Control Board (CCB):** includes representatives from each of the major stakeholders, who evaluate requested changes to the ALMR system and identify possible impacts and the risks associated with them.

**CI:** Controlled Interface

**CIO:** Chief Information Officer

**CND:** Computer Network Defense

**CNDSP:** Computer Network Defense Service Provider

**CPU:** Central Processing Unit



*Alaska Land Mobile Radio Communications System  
Security Controls Review Procedure 200-6*

**COMSEC:** Communications Security

**COTS:** Commercial Off the Shelf

**CSSP:** Cybersecurity Service Provider, replaced Computer Network Defense Service Provider (CNDSP) IAW DoD Manual 8530.01, Cybersecurity Activities Support Procedures protect the DoD Information Network (DoDIN).

**Cybersecurity:** 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 Defense (DoD) – Alaska:** Alaskan Command, US Air Force and US Army component services, operating under United States Pacific Command and United States Northern Command.

**Department of Defense Information Network (DoDIN):** The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

**Department of Public Safety (DPS):** a State of Alaska (SOA) department where the SOA Telecommunications System (SATS) and ALMR programs reside.

**DES:** Data Encryption Standard

**DISA:** Defense Information Systems Agency

**DMZ:** Demilitarized Zone

**DNS:** Domain Name Server

**DRP:** Disaster Recovery Plan

**DSA:** Digital Signature Algorithm

**EAL:** Evaluation Assurance Level

**ECDSA:** Elliptic Curve Digital Signature Algorithm



## *Alaska Land Mobile Radio Communications System Security Controls Review Procedure 200-6*

**Enterprise Mission Assurance Support Service (eMASS):** a government owned web-based application with a broad range of services for comprehensive fully integrated cybersecurity management.

**EMSEC:** Emanations Security

**Executive Council:** governing body 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).

**FIPS:** Federal Information Processing Standard

**FISMA:** Federal Information Security Management Act

**FSO:** File System Object

**GIG:** Global Information Grid

**GOTS:** Government Off the Shelf

**HIPAA:** Health Insurance Portability & Accountability Act

**IAV:** Information Assurance Vulnerability

**IAVA:** Information Assurance Vulnerability Alert

**IAVB:** Information Assurance Vulnerability Bulletins

**IAVM:** Information Assurance Vulnerability Management

**IAVTA:** Information Assurance Vulnerability Technical Advisors

**IDS:** Intrusion Detection System

**Information Systems Security Manager (ISSM):** the individual responsible for establishing and maintaining security controls that ensure the availability, confidentiality, and integrity of the ALMR system under the Risk Management Framework (RMF).

**Member:** a public safety agency including, but not limited to, a general government agency (local, state, tribal, or federal), its authorized employees and personnel (paid or volunteer), and its service provider, participating in and using the system under a membership agreement.



## *Alaska Land Mobile Radio Communications System Security Controls Review Procedure 200-6*

**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.

**NIAP:** National Information Assurance Partnership

**NIPRNET:** Non-classified Internet Protocol Router Network

**NIST:** National Institute of Standards and Technology

**NSA:** National Security Agency

**NSTISSP:** National Security Telecommunications and Information Systems Security Policy

**NTFS:** New Technology File System

**OS:** Operating System

**PKE:** Public Key Encryption

**PKI:** Public Key Infrastructure

**POA&M:** Plan of Action & Milestones

**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 manage information security risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, the Nation, and includes: (1) establishing the context for risk-related activities; (2) assessing risk; (3) responding to risk once determined; and (4) monitoring risk over time. The program 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.

**RSA:** a security algorithm used for signing an encryption presented by Rivest, Shamir, Adleman (RSA).

**S/MIME:** Secure Multipurpose Internet Mail Extensions

**SAMI:** Sources and Methods Intelligence

**SAN:** Storage Area Network



*Alaska Land Mobile Radio Communications System  
Security Controls Review Procedure 200-6*

**SCA:** Security Controls Assessor

**SIPRNET:** Secure Internet Protocol Router Network

**SISO:** Senior Information Security Officer

**SNAC:** Single Network Access Code

**SOP:** Standard Operating Procedure

**SRG:** Security Recommendation Guide

**SSH:** Secure Shell

**SSL:** Secure Socket Layer

**State of Alaska (SOA):** the primary maintainer of the state's infrastructure system, and shared owner of the system. The State of Alaska sponsors local/municipal agencies onto the system.

**STIG:** Security Technical Implementation Guides

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

**TEMPEST:** is an unclassified U.S. government code word for compromising emanations.

**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. All terms and conditions of the Cooperative and Mutual Aid agreement defined apply to local/municipal government agencies that are sponsored/represented by the State of Alaska.

**User Council:** governing body 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.

**UNIX:** Uniplexed Information and Computing System





*Alaska Land Mobile Radio Communications System  
Security Controls Review Procedure 200-6*

**VoIP:** Voice-over Internet Protocol

**VPN:** Virtual Private Network

**VTC:** Video Teleconferencing

**WAN:** Wide Area Network



## **1.0 Purpose**

The Alaska Land Mobile Radio (ALMR) Communications System Security Controls Review provides evidence of compliance with applicable laws, directives, policies, and requirements regarding information security. It examines and analyzes the security safeguards of the system to ensure that appropriate security procedures have been developed and implemented.

This procedure describes how the system will be tested, evaluated, and validated against in-place mechanisms that protect sensitive information processed, produced, stored, and/or transmitted on the network. This Security Controls Review is limited to the system and its operating environment.

## **2.0 References**

The following documents were used in the preparation of this document.

- a. Department of Defense (DoD) Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DoD Systems
- b. Committee on National Security Systems Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems
- c. Federal Information Security Management Act (FISMA) of 2002 Chapter 32, Subchapter III

## **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 Security Controls Review Procedure warrant such action.

### **3.2 User Council**

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

### **3.3 Information Systems Security Manager**

The Information Systems Security Manager (ISSM) shall oversee the Security Controls Review completion and provide an informal briefing to the Operations Manager and the System Manager on the findings at least annually.



## **4.0 Security Controls Review Planning**

### **4.1 Review Objectives and Requirements**

The Risk Management Framework (RMF) for DoD Information Technology (IT) includes the development of an authorization package for the system.

The requirements for RMF are based upon existing federal, state, and local government security requirements, as well as ALMR functional requirements, industry standards, and industry best practices for security in the field of radio communications.

These policies translate the broad range of threats to radio systems into general protection policies and requirements.

### **4.2 Information and Resources Under Review**

The information and resources upon which this Security Controls Review shall be conducted includes all the documentation and facilities supporting the system, including maintenance and configuration control. The information and resources are detailed in the following paragraphs.

#### **4.2.1 Documentation and Information Resources**

The following documentation will be required for conducting the Security Controls Review:

- List of RMF controls to assess during annual FISMA review.
- All ALMR documents and artifacts in Enterprise Mission Assurance Support Service (eMASS).
- Current RMF eMASS Authorization to Operate (ATO) Package.
- Personnel rosters (access lists).
- Physical security inspections.
- Current Vulnerability scans and STIG results for ALMR components.

#### **4.2.2 Facility Resources**

The rooms where the system is installed will be tested through inspection to ensure the appropriate non-technical safeguards protect the information and resources from unauthorized disruption, disclosure, modification, and/or denial of service.



### **4.2.3 Maintenance and Configuration Control Resources**

The system maintenance and configuration control procedures will be assessed through inspection and/or analysis to determine compliance with security policy objectives and/or security requirements.

## **5.0 Assumptions**

For the purposes of this annual Security Controls Review Procedure, the following assumptions have been made:

- The results of pre-testing (conducted with the Security Controls Validation Worksheets) will be consistent with observations and tests made on site.
- The system will undergo the Security Controls Review with completion to roughly coincide with the functional testing.
- System security administration staffing will be identified and appointed, as necessary, and as additional agencies become part of ALMR.

## **6.0 Approach to Security Controls Review**

In accordance with the Air Force implementation of RMF, the annual control review will be conducted as part of the FISMA review. Each year, there will be a 100 percent review of existing control assessment results in eMASS, and new assessments will be conducted on 100 percent of the Category I controls, 50 percent of the Category II controls, and 25 percent of the Category III controls. The specific Category II and III controls will differ each year to ensure 100 percent of all ALMR RMF controls are reassessed over the three-year life cycle of the ATO.

The controls will be assessed against the descriptions and assessment procedures identified within eMASS for each control and associated Control Correlation Identifiers (CCI). Assessment results will be uploaded into eMASS by the ALMR ISSM(s) and moved through the eMASS Control Approval Chain (CAC) to facilitate validation by the government Security Control Validator (SCV). Generally, compliance with the security requirements may be verified or validated by the following methods:



## Alaska Land Mobile Radio Communications System Security Controls Review Procedure 200-6

EVALUATION METHOD	DESCRIPTION	INCLUDED IN IA CONTOL VALIDATION WORKSHEETS	INCLUDED IN TEST CASE WORKSHEETS
<b>Analysis</b>	Verifying compliance with requirements through evaluation using recognized analytical techniques, such as comparing design with requirements. Conducted prior to executing the on-site Security Controls Review.	<b>X</b>	
<b>Inspection</b>	Validating compliance with requirements by physically examining or reviewing a feature, either through observation or interviews with relevant personnel. Can be conducted prior to or during the execution of the Security Controls Review.	<b>X</b>	
<b>Documentation</b>	Validating compliance with requirements by reviewing relevant documentation. Can be conducted prior to or during the execution of the Security Controls Review.	<b>X</b>	
<b>Test</b>	Validating compliance with requirements by collecting, analyzing, and evaluating data through systematic hands-on measurement under appropriate conditions. Conducted during the execution of the Security Controls Review.		<b>X</b>

### 6.1 Execution of Security Controls Review

During the FISMA review process, the ALMR ISSM(s) will coordinate/communicate with the ALMR technical and operations personnel to collect any information or supporting documentation required during the assessment process. Any new non-compliant controls will require creation of vulnerabilities for the control as well as establishment of a Plan of Action and Milestones (POA&M) item in eMASS to include description, risk, mitigation, and milestone date.

The annual FISMA review also requires a review and testing of the ALMR Contingency Plan. The review of the plan can be documented in the change history of the plan and a signed memo by the ALMR Program Manager (PM) indicating when the plan review was completed. The testing of the Contingency Plan may be a tabletop exercise with meeting minutes describing the test scenario, participants, summary of whether the key personnel knew and performed their respective roles, and any lessons learned. The other option is to use a real-world contingency that occurred during the past year and document it to include the same type of information identified in the above description for the tabletop exercise. Documentation of the plan review and testing will be uploaded into eMASS as part of the validation that the FISMA review was completed.

### 6.2 Document Review Results

The annual FISMA process is documented within the living RMF eMASS instance for ALMR. If required, the ALMR ISSM(s) can export an RMF Scorecard and POA&M and provide via email to the Operations Manager and System Manager, if requested.



## *Alaska Land Mobile Radio Communications System Security Controls Review Procedure 200-6*

Typically, the PM, SCV, and Authorized Official (AO) will be aware of the FISMA review results and will not require a debriefing.

### **7.0 Compliance**

Compliance with the Security Controls Review Procedure is outlined in ALMR Security Controls Review Policy Memorandum 200-6.