Alaska Land Mobile Radio Communications System

Security Controls Review Procedure 200-6

Version 8

December 13, 2016

Developed through contract with:

Table of Contents

Document Revision History

Name	Date	Reason for Changes	Version
Shafer, Sherry	4/20/2009	Approved by the User Council – Final.	1
Shafer, Sherry	4/30/2010	Annual review/update. Approved by the User Council - Final.	2
Shafer, Sherry	5/9/2011	Annual review/update. Approved by the User Council - final.	3
Shafer, Sherry	8/24/2012	Annual review/update. Approved by the User Council - final.	4
Shafer, Sherry	9/3/2013	Annual review/update; approved by the Operations Management Office - final.	5
Shafer, Sherry	9/18/2014	Annual review/update; approved by the Operations Management Office - final.	6
Shafer, Sherry	9/8/2015	Annual review/update. Approved by the Operations Management Office - final.	7
Shafer, Sherry	12/13/2016	Annual review/update. Approved by the User Council – final.	8

Acronyms and Definitions

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. The ALMR System is a digital, trunked, wide-area network (WAN), shared system between the Department of Defense (DOD), the Federal Executive Association (FEA) of Alaska (excluding DOD), the State of Alaska (SOA), the Alaska Municipal League, and the Municipality of Anchorage.

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

ADP: automated data processing

AES: advanced encryption standard

AIS: automated information system(s)

C3I: command, control, communications, and intelligence

CAC: common access card

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

COMSEC: communications security

COTS: commercial off the shelf

CSSP: Cybersecurity Service Provider, replaced Computer Network Defense Service Provider (CNDSP) IAW DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations.

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 – 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 set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

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

EMSEC: emanations security

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).

Federal Executive Association (FEA): federal government entities, agencies and organizations, other than the Department of Defense, that operate on the shared ALMR system infrastructure.

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

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.

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 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 years.

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

S/MIME: secure multipurpose internet mail extensions

SAMI: Sources and Methods Intelligence

SAN: Storage Area Network

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 SATS (the State's microwave system), and shared owner of the System.

STIG: security technical implementation guides

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.

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

User/Member: an agency, person, group, organization or other entity which has an existing written Membership Agreement with one of the Parties to the 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 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.

UNIX: uniplexed information and computing system

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 Instruction (DODI) 8510.01, Risk Management Framework(RMF) for DoD Information Technology (IT)
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 Security Manager

The Security Manager (SCM) shall oversee the Security Controls Review completion and provide a report for presentation to the UC and EC on the findings.

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 of 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:

- FISMA Checklist and instructions for completing the checklist
- All ALMR System policies and procedures
- Current Authority to Operate (ATO) Package
- Security Controls that are defined as applicable to the ALMR System in accordance with CNSSI 1253
- Personnel rosters (access lists)
- Physical security inspections
- Vulnerability scans of ALMR information systems

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 though inspection and/or analysis to determine compliance with security policy objectives and/or security requirements.

5.0 Assumptions

For the purposes of this 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 at the same time it undergoes 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

Each Security Control will be tested to ensure compliance by completing the applicable Security Controls Validation Worksheets. Generally, compliance with the security requirements may be verified or validated by the following methods:

EVALUATION METHOD	DESCRIPTION	INCLUDED IN IA CONTOL VALIDATION WORKSHEETS	INCLUDED IN TEST CASE WORKSHEETS
Analysis	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.	**X**	
Inspection	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.	**X**	
Documentation	Validating compliance with requirements by reviewing relevant documentation. Can be conducted prior to or during the execution of the Security Controls Review.	**X**	
Test	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.		**X**

6.1 Execution of IA Control Review

The Security Controls Review will be conducted at System facilities on-site. The worksheets will be used to inspect and/or analyze the capabilities of the System and its environment in support of certifying the ALMR System. In addition, the Security Controls Validation Worksheets will also be used to verify any items left open after the pre-test evaluation.

The Security Controls Review Team will decide which specific ALMR sites and equipment will be tested and evaluated. In general, it is not logistically practical to test every facility and piece of equipment in the System. For the Security Controls Review, a representative sample of sites and equipment from each portion of the System will be selected for Security Control Review activities.

Deviations from the "Expected Results" in each worksheet will be assessed to consider whether the test step was invalid or if the test step exhibited a failure to comply with the security objective and associated requirement.

After completion of the Security Controls Validation Worksheets, they will be marked either "Compliant", or “Non-Compliant. If any part of the test case fails to provide the "Expected Results", the worksheet will be marked as "Non-Compliant" and descriptive comments must be recorded in the worksheet’s “Non-Compliant Impact Statement” section.

6.2 Document Review Results

An annual Security Controls Review Report shall be created, which documents the findings of an assessment of a subset of implemented security controls reflective of the security categorization of the System and any threats to the System.

During reauthorization, an annual Security Controls Review Report shall be created, which documents the findings of the Security Controls Review. This report shall consist of all completed Security Controls Validation Worksheets, as well as a completed RMF Scorecard and POA&M Report as described in (DODI) 8510.1. The report will provide a statement of the security requirements to which the System does not comply and a summary of observed non-compliance.

7.0 Debrief IA Control Review Results

At the conclusion of Security Controls Review activities, the Security Controls Review Team will provide an informal briefing of the results of the Security Controls Review to the Operations Manager and the System Manager.

The SCM will work to rectify areas of non-compliance prior to the development of the Security Controls Review Report. The draft Security Controls Review Report will be subsequently developed and provided to the System Manger for review.

Following feedback from the System Manager, the annual Security Controls Review Report will be finalized and submitted through the Authorizing Official (AO) as supporting documentation for an Authorization Decision (AD)

8.0 Retesting

Should there be any "Non-Compliant" test cases, the SCM will have the opportunity to assess the value of correcting the finding (i.e., in terms of cost, perceived risk, certification requirements, etc.), implement a correction and submit the System to regressive re-testing at the discretion of the Security Controls Assessor (SCA).

9.0 IA Control Review Execution

Security Controls Review execution will be conducted using the Security Controls Validation Worksheets and recorded in eMASS, as well.

9.1 Worksheet Structure

The structure of the Security Controls Validation Worksheets, as well as a brief description of each form field, follows:

9.2 Worksheet Execution

Observed validation results will be compared to the expected results identified in each Security Controls Validation Worksheet. The test procedure will be subjectively rated and any comments documented. Additional tests may be conducted at the discretion of the reviewer to clarify validation results and meet Security Controls objectives.

Completion of the worksheets provides the data upon which the System will be evaluated to determine compliance with RMF requirements.

10.0 Compliance

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