Alaska Land Mobile Radio Communications System

Security Controls Review Procedure 200-6

Version 10

December 19, 2018

Developed through contract with:

Bering Straits Information Technology, LLC
A Subsidiary of the Bering Straits Native Corporation

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
Shafer, Sherry	12/27/2017	Annual review/update. Approved by the Operations Management Office - final.	9
Shafer, Sherry	12/19/2108	Annual review/update. Approved by the Operations Management Office - final. Del Smith 12.19.18	10

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 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

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 RMF.

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 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 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.

Member: an agency, person, group, organization or other entity which has an existing written Membership Agreement with one of the Parties to the Cooperative and Mutual 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 (DOD) 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 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 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:

- List of RMF controls to assess during annual FISMA Review
- All ALMR documents and artifacts in 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 though 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:

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 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 table top 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 table top 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.

Typically the PM, SCV and 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.