Alaska Land Mobile Radio Communications System

System Incident Response Procedure 400-2

Version 11

September 16, 2019

Table of Contents

Document Revision History

Name	Date	Reason for Changes	Version
Shafer, Sherry	12/22/2008	Approved by the User Council – Final.	1
Shafer, Sherry	12/21/2009	Annual review/update. Approved by the User Council – Final.	2
Shafer, Sherry	2/23/2011	Annual review/update. Approved by the User Council - final.	3
Shafer, Sherry	9/10/2012	Annual review/update. Approved by the User Council - final.	4
Shafer, Sherry	9/4/2013	Annual review/update; approved by the Operations Management Office - final.	5
Shafer, Sherry	9/24/2014	Annual review/update. Approved by the Operations Management Office – final.	6
Shafer, Sherry	9/23/2015	Annual review/update. Approved by the Operations Management Office – final.	7
Shafer, Sherry	9/12/2016	Annual review/update. Approved by the Operations Management Office – final.	8
Shafer, Sherry	9/12/2017	Annual review/update. Approved by the Operations Management Office – final.	9
Shafer, Sherry	9/17/2018	Annual review/update. Approved by the Operations Management Office – final.	10
Shafer, Sherry	9/16/2019	Annual review/update. Approved by the Operations Management Office – final.	11

Acronyms and Definitions

Alaska Federal Executive Association (AFEA): federal government entities, agencies and organizations, other than the Department of Defense, that will 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 Alaska Public Safety Communications Service (APSCS), as established in the Cooperative and Mutual Aid Agreement.

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

Alaska Public Safety Communications Service (APSCS): the State of Alaska statewide telecommunications system microwave network.

Cooperative and Mutual Aid Agreement: the instrument that establishes ALMR and sets out the terms and conditions by which the system will be governed, managed, operated and modified by the Parties signing the Agreement.

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 Administration (DOA): a State of Alaska (SOA) department that maintains the Alaska Public Safety Communications Service (APSCS) 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.

DODI: Department of Defense Instruction

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 Information Security Management Act of 2002 (**FISMA**)**:** a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.

L.107-347, 116 Stat. 2899). The Act was meant to bolster computer and network security within the Federal Government and affiliated parties (such as government contractors) by mandating yearly audits.

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.

Impact: The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.

Impact Level: The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Incident: An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. See cyber incident. See also event, security-relevant, and intrusion.

Incident Response Team (IRT): a specialized team, comprised of ALMR staff and technical specialists, activated at the request of the Security Manager to investigate a System incident.

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

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 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.

National Institute of Standards and Technology (NIST): non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

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.

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.

State of Alaska (SOA): the primary maintainer of the State's 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: 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 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 to define roles and responsibilities of an Incident Response Team (IRT) for the Alaska Land Mobile Radio (ALMR) Communications System, describes the operational requirements for that team and authorizes that team to take action on behalf of ALMR.

2.0 Roles and Responsibilities

2.1 Executive Council

2.1.1 The Executive Council (EC) is granted authority through the ALMR Cooperative and Mutual Aid Agreement to take necessary actions to protect the ALMR System. The EC has the following specific responsibilities:

- Approve and oversee information security control techniques to address System incident planning
- Assist senior agency officials with their responsibilities for System incident response
- Review all efforts and responses for documented incidents

2.1.2 The EC shall also be responsible for the management and enforcement of sanctions when violations of the Security Incident Response Procedure warrant such action.

2.2 User Council

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

2.3 Operations Management Office

The Operations Management Office (OMO) will review all available information regarding Severity 1 or 2 events (see Section 4) and make a determination on whether or not to notify the EC or UC. Normally, notifications will be provided via email.

2.4 System Management Office

2.4.1 The System Management Office (SMO) shall maintain escalation lists, contact lists, process flows, lists of subject matter experts and configuration procedures for the System.

2.4.2 To ensure the appropriate level of support can be obtained during a System incident, the SMO shall require all vendors and user agencies participating on the

System to provide incident response points of contact, and an internal means to initiate immediate contact.

2.4.3 In the event of a System incident discovered by the SMO, the SMO shall:

- Notify the appropriate personnel as defined in Table 4-4
- Assist in determining the existence and severity level of the incident, in accordance with these procedures, and activate the IRT, if necessary
- Notify affected System users
- Participate as members of the IRT and assist in resolving the incident
- Procure and coordinate all additional resources required to resolve the incident

2.5 Information Systems Security Manager

2.5.1 The ALMR Information Systems Security Manager (ISSM) is responsible for ensuring an appropriate operational security posture is maintained for an information system or program. The ISSM has operational authority for specified information, and is responsible for identifying the controls for information generation, collection, processing, dissemination and disposal.

2.5.2 The ISSM shall:

- Review and/or update the ALMR System Incident Response Procedure, at least annually
- Ensure monitoring and configuration controls are in place to properly notify the appropriate agencies/individuals of a System security incident
- Automate the monitoring of systems to provide prompt incident notification, where possible
- Create and maintain an incident history database that retains incident related data, in accordance with this procedure

2.5.3 In the event of a System security incident discovered by the ISSM, he/she shall:

- Notify the appropriate personnel as defined in Table 4-4
- Assist in determining the existence and severity level of the incident, in accordance with this procedure, and activate the IRT, if necessary
- Participate as a member of the IRT and assist in resolving the incident
- Provide detailed incident documentation and reporting as outlined in this procedure
- Report critical security incidents to both the OMO and the Authorizing Official (AO)
- Oversee the IRT to ensure:
  - Proper coordination takes place for all incident response efforts

- All actions taken in response to an incident do not compromise the required integrity and availability of the System
- System users and support personnel are properly notified of the incident
- Response efforts maintain the required Security Controls for system security impact levels of low confidentiality, moderate integrity and moderate availability
- Detailed documentation and reports are created and delivered in accordance with this procedure

2.6 System Administrators, Technicians, and Users

2.6.1 System administrators and technicians (privileged users) should perform the following activities when there is a suspicion that an incident has occurred:

- Identify any potential security incident
- Report the potential security incident to the System Manager or ISSM
- Preserve any forensic evidence (do not delete or edit files, and preserve time stamps)
- Secure any affected equipment
- Participate as a member of the IRT
- Perform other appropriate tasks, as annotated in ALMR Privileged User Acceptable Use Procedure 400-7

2.6.2 The user role encompasses both handset and console operators across many organizations, including DOD, Federal Non-DOD, State, local and even private sector personnel.

For the current ALMR System, handset users do not have data access to the ALMR network, and as such, have no cybersecurity responsibilities beyond user awareness and reporting of potential cybersecurity incidents.

Console operators have additional responsibilities to notify the SMO, preserve forensic evidence and secure affected equipment in the event of a cybersecurity incident (see Privileged User Acceptable Use Procedure 400-7).

3.0 Incident Response Team

A team will be activated when an incident occurs, in accordance with guidelines outlined in this procedure. The IRT will determine the impact of an incident, the required corrective actions, perform root cause analysis and generate incident reports.

3.1 Administration

The SMO is responsible for maintaining and distributing the administrative documents that support and define the IRT. These documents include escalation lists, contact lists, process flows, lists of subject matter experts and the procedures used by the IRT.

3.2 Membership

The IRT shall consist of the Operations Manager, System Manager, ISSM, applicable technical subject matter experts, vendors and member organization representatives. The ISSM and SMO shall coordinate efforts to ensure an IRT, with the appropriate skill and expertise, is convened for each System incident.

3.3 Activation

In coordination with the Operations Manager and the System Manager, the ISSM shall contact and activate the IRT.

3.4 Deactivation

The IRT will be deactivated once it has been determined that the incident has been resolved, an After Action Review has been completed and incident reports created.

4.0 Incident Detection and Analysis

4.1 Incident Severity Matrix

Severity of an incident is based on the impact to the System. The impact of an incident is assessed using one of two criteria:

- Incidents that affect the availability of the System
- Incidents that affect the confidentiality or integrity of the data within the System

A System incident is defined as any adverse event threatening the confidentiality, integrity or availability of ALMR information assets, information systems and supporting networks.

Adverse events may include the insertion of malicious code (e.g. viruses, Trojan horses or backdoors), unauthorized or unapproved scans or probes, successful and unsuccessful intrusions and insider attacks. Any violation of ALMR formal security policies, or acceptable use policies, is also defined as an incident.

The following matrix defines the assessed severity levels of security incidents on the ALMR System.

Severity	Threat	Incident Measurement Criteria
Severity 1 Critical	Operation	**Subsystem Impacted – Major System Failure.** Master Site zone controller, Category 1 RF Sites*, Category 2 RF Sites**, Category 3 RF Sites***, management terminals used for maintenance, System Gateways, and Vendor maintained microwaves.
	Data	Controlled system administration data or voice communications disclosed or altered without authorization.
Severity 2 High	Operation	**Subsystem Impacted – Significant System Impairment and Intermittent Problems.** Master Site zone controller, Category 1 RF Sites, Category 2 RF Sites, Category 3 RF Sites, and Management Terminals used for maintenance, System Gateways, and Vendor maintained microwaves.
	Data	An incident has occurred in which it cannot be determined if controlled system administration data or voice communications have been disclosed or altered without authorization. Loss of multiple handsets that are known or suspected to be in the hands of unauthorized users.
Severity 3 Medium	Operation	**Parts, Upgrades, Intermittent problems, Issues Currently Under Observation.** An issue that does not preclude use of the system, sub-system, or critical features. Failure of or loss of connectivity of no more than one site within the ALMR network.
	Data	An incident has occurred, which if not addressed, may result in controlled system administration data or voice communications being disclosed or altered without authorization in the future. Multiple security policy violations with potential or actual impact to operations or data integrity. Loss of multiple handsets.
Severity 4 Low	Operation	**Scheduled Maintenance.** Scheduled maintenance and upgrades.
	Data	Loss of a single handset. A single security policy violation with potential or actual impact to operations or data integrity.

*Category 1 – A critical site within 30 miles of a military base, Anchorage, Fairbanks, Juneau, Palmer/Wasilla, Soldotna/Kenai, or any site so designated
**Category 2 – Other drive-to sites – not critical
***Category 3 – Helicopter (helo.) sites (some helo. sites are classified as Category 1)

Table 4-1. Incident Severity Matrix

4.2 Incident Categories

Incidents can occur in many ways, making it impractical to develop comprehensive procedures with step-by-step instructions for handling every incident. The best approach is to prepare to handle any type of incident by grouping incidents into general categories. The incident categories listed in Table 4-2 are defined by the United States Computer Emergency Readiness Team (US-CERT) for use throughout the Federal government and supported organizations.

Category	Name	Description
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.
CAT 1	*Unauthorized Access	An individual gains logical or physical access without permission to an agency network, system, application, data, or other resource
CAT 2	*Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
CAT 3	*Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.
CAT 4	*Improper Usage	A person violates acceptable computing use policies.
CAT 5	Scans/Probes/Attempted Access	Any activity that seeks to access or identify an agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or DoS.
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

*Defined by NIST Special Publication 800-61

Table 4-2. Incident Categories

4.3 Incident Detection

Signs of an incident fall into one of two categories:

- Indication - a sign that an incident may have occurred or may be occurring
- Precursors - a sign that an incident may occur in the future

There are many vectors through which signs of an incident can be detected. The following table lists the probable methods of detection for defined categories of incidents, as defined for Federal organizations by US-CERT.

Category	Name	Probable Method of Detection
CAT 0	Exercise/Network Defense Testing	• Planned, official notification
CAT 1	*Unauthorized Access	• Physical security sensors or logs • Direct observation • Motorola® Security Operations Center notification
CAT 2	*Denial of Service (DoS)	• Motorola® Security Operations Center notification • End user notification • System administrator
CAT 3	*Malicious Code	• Motorola® Security Operations Center notification
CAT 4	*Improper Usage	• Direct observation
CAT 5	Scans/Probes/Attempted Access	• Motorola® Security Operations Center notification
CAT 6	Investigation	• Motorola® Security Operations Center notification

*Defined by NIST Special Publication 800-61

Table 4-3 Probable Incident Detection Methods

It is important to note that while the Motorola® Security Operations Center will serve as the probable primary detection point for many of the categories of incidents listed above, there are other possible methods of detecting an incident on the ALMR System. All detected incidents should be reported using the same notification and response processes.

4.4 Incident Response

When an incident has been detected, both the System Manager and ISSM shall be notified. Upon validation of the legitimacy of the incident by either the System Manager or the ISSM, the IRT shall be activated. The incident shall be prioritized by the IRT.

The IRT shall work quickly to analyze and validate each incident, documenting each step taken. The team will rapidly perform an initial analysis to determine the incident scope (e.g. which networks, systems or applications are affected), who or what originated the incident, and how the incident is occurring (e.g. what tools or attack methods are being used or what vulnerabilities are being exploited).

The initial analysis will provide enough information for the IRT to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident. When in doubt, incident handlers will assume the worst until additional analysis indicates otherwise. All facts regarding the incident should be recorded in an ongoing incident log.

4.5 Incident Notification

The following table lists the top-level notification contacts for the incident severities established in Table 4-1.

Severity	Notification Required to be Provided to:
Severity 1 Critical	Operations Management Office System Management Office Information Systems Security Manager
Severity 2 High	Operations Management Office System Management Office Information Systems Security Manager
Severity 3 Medium	System Management Office Information Systems Security Manager
Severity 4 Low	System Management Office Information Systems Security Manager

Table 4-4. Notification Contacts by Severity

The notification timeframes listed in the Incident Notification Matrix below are the specified timeframes for notification of US-CERT for Federal organizations. Internal ALMR notification timeframes should not exceed those listed in the table.

Category	Name	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	Daily **NOTE:** Within one (1) hour of discovery/ detection, if widespread across agency.
CAT 4	*Improper Usage	Weekly
CAT 5	Scans/Probes/Attempted Access	Monthly **NOTE:** If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	Not Applicable. This category is for each agency's use to categorize a potential incident that is currently being investigated.

*Defined by NIST Special Publication 800-61

Table 4-5. Incident Notification Matrix

4.6 Reporting

The following sections describe the reports, records and communications required for incident response efforts.

4.6.1 Incident Response Minutes

The IRT shall assign a note keeper for all incident response meetings to record the meeting minutes. These minutes will be distributed, at a minimum, to the entire active IRT and the Operations Manager. The minutes will be stored as a formal record with the final incident report, along with any retained evidence data.

4.6.2 Incident Declaration Report

The Incident Declaration Report will be distributed to the OMO by the IRT for all Severity I and II incidents. This report will serve as a formal notification of the incident and will describe:

- The nature of the incident
- The impact of the incident
- Any temporary actions needed to minimize operational impact
- The estimated time until incident resolution

4.6.3 Incident Status Update Report

Regular update reports will be provided to the OMO and the active IRT for all Severity I and II incidents. The IRT will determine if the reporting interval must be changed to accommodate the circumstances of a specific incident.

Unless otherwise dictated by the IRT, the status reporting intervals described in Table 4-6 shall be used.

Severity	Update Interval
Critical (1)	Every four hours, until resolution
High (2)	Daily until resolution

Table 4-6. Incident Status Update Intervals

4.6.4 Third-Party Incident Reporting Organizations

ALMR must report specific incidents, as defined in Federal Information Security Management Act (FISMA) requirements (see NIST SP800-61), to the US-CERT center. The defined categories for incidents are listed in Table 2 and the timeframes for reporting incidents are listed in Table 4-5.

As per US-CERT, reports of computer incidents should include a description of the incident or event, using the appropriate category and as much of the following information as possible. However, reporting should not be delayed in order to gain additional information.

- Agency name
- Point of contact information including name, telephone, and email address
- Incident Category Type (per Table 4-2)
- Incident date and time, including time zone
- Source IP, port, and protocol
- Destination IP, port, and protocol
- Operating System, including version, patches, etc.
- System Function (e.g. server, workstation, etc.)
- Antivirus software installed, including version, and latest updates
- Location of the system(s) involved in the incident
- Method used to identify the incident (e.g. IDS, audit log analysis, system administrator)
- Impact to agency/System
- Resolution

All IRT members should utilize this schema when reporting incidents to the US-CERT. Depending on the criticality of the incident, it is not always feasible to gather all the information prior to reporting. In this case, the IRT should continue to report information as it is collected. (US-Cert Incident Report Site: https://forms.us-cert.gov/report/)

4.6.5 Incident Conclusion Report

An Incident Conclusion Report shall be completed by the IRT within two business days of the conclusion of an incident response effort. The report will describe:

- An executive summary of the incident
- The timeline of the incident
- The nature of the incident
- The operational impact of the incident
- How the incident was identified
- Corrective action(s) taken to restore the System to its pre-incident condition
- Recommended sanctions, if applicable

4.6.6 After Action Review

An After Action Review (AAR) of the response effort shall be completed within 30 days of the conclusion of an incident response effort. The AAR will examine the effectiveness of the incident response activity, identify any areas requiring improvement and any sanctions imposed by the EC. All participating IRT members shall be provided an opportunity to provide input during this process. Areas to be considered during this review include:

- Speed, accuracy and completeness of incident detection
- Speed, accuracy and completeness of incident containment
- Speed, accuracy and completeness of incident recovery
- Effectiveness of procedures utilized during the response effort
- Any procedural gaps requiring correction
- Any complicating factors that affected the incident response effort

The report shall describe the collective opinions of the participants of the review. The IRT shall provide this report to the OMO.

4.7 Incident Record Retention

Records of the incident must be stored in a secure and accessible location. The ISSM shall maintain a System incident history database which includes, meeting minutes, reports, logs and other related information for all System incidents. Stored data must be tamper resistant.

4.8 External Information Sharing

Any information about the ALMR System, its personnel, its capabilities, its physical location(s), software and hardware specifications, or any privileged aspect of the System or its resources, may not be disseminated to "outside entities" without written permission of the EC.

The nature of a given incident 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 ISSM, and approved in writing by the EC.

4.9 Public Media Disclosure

The ALMR System has a security impact of Moderate Confidentiality, Moderate Integrity and Moderate Availability. 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).

4.9.1 Written approval by the ISSM, SOA Office of Information Technology (OIT) Director and the Alaskan Command J6, must be obtained before any information relative to incidents involving the ALMR System is released to public media, as outlined in ALMR Records Management Procedure 300-1, paragraph 6.5, Release of Records.

4.9.2 Law Enforcement. In the event that law enforcement involvement is required to mitigate a System incident, the ISSM shall serve as the primary contact for law enforcement. While disclosure of a security incident is not required to be made public under FOIA, once information has been submitted as evidence in a court proceeding, it may not be excluded from FOIA.

5.0 Incident Response Testing

The ALMR System incident response plan will be tested on an annual basis in accordance with section 3 of this document. This testing will be accomplished as a table top exercise and documented as thought it were an actual incident. The Incident Conclusion Report and After Action Review will be retained in accordance with requirements in section 4.7 of this document.

6.0 Compliance

Compliance with the System Incident Response Procedure is outlined in ALMR System Incident Response Policy Memorandum 400-2.

Reference Documents

1. NIST SP800-61r2, Computer Security Incident Handling
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

2. NIST SP800-100, Information Security Handbook: A Guide for Managers
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

3. NIST SP800-53r4, Recommended Security Controls for Federal Information Systems
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

4. NIST SP800-52r1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

5. NIST SP800-12r1, An Introduction to Computer Security
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

6. DODI 8510.01CH2, Risk Management Framework (RMF) for DOD Information Technology (IT)
http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf