Security Authorization Process Guide

Office of the Chief Information Security Officer (CISO)

Version 11.1

March 16, 2015

TABLE OF CONTENTS

Introduction ... 1
1.1 Background ... 1
1.2 Purpose ... 2
1.3 Scope ... 2
2.0 Roles and Responsibilities ... 2
2.1 Authorizing Official (AO) ... 2
2.2 Chief Information Security Officer (CISO)/Information System Security Manager (ISSM) ... 3
2.3 DHS Inventory Team ... 3
2.4 Security Control Assessor (SCA) ... 4
2.5 Security Authorization Team ... 5
2.6 Information System Security Officer (ISSO) ... 5
2.7 System Owner ... 6
2.8 Business Owner ... 6
2.9 Program Manager ... 6
2.10 Technical staff ... 6
2.11 Privacy Office ... 7
2.12 DHS Document Review Team (DR) ... 7
3.0 Risk Management Framework ... 7
3.1 Categorize ... 7
3.2 Select ... 9
3.3 Implement ... 10
3.4 Assess ... 12
3.5 Authorize ... 13
3.6 Monitor ... 15
4.0 Ongoing Authorization ... 15
5.0 Cloud and FEDRAMP Authorizations ... 16
Appendix A: References ... A1

INTRODUCTION

Under the authority of the Department of Homeland Security (DHS) Chief Information Officer (CIO), the Chief Information Security Officer (CISO) bears the primary responsibility to ensure compliance with Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB), and all applicable laws, directives, policies, and directed actions on a continuing basis. This document sets forth the DHS Security Authorization process of information systems operated within the Department.

1.1 BACKGROUND

Security authorization (SA) is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. The Authorizing Official (AO) accepts security responsibility for the operation of an assessed system and officially declares that it is authorized to operate.

Security authorization involves comprehensive testing and evaluation of security features (also known as controls) of an information system. It addresses software and hardware security safeguards; considers procedural, physical, and personnel security measures; and establishes the extent to which a particular design (or architecture), configuration, and implementation meets a specified set of security requirements throughout the life cycle of the information system. It also considers procedural, physical, and personnel security measures employed to enforce information security policy.

An information system must be granted an Authority to Operate (ATO) before it first becomes operational, and must be re-authorized at least every three (3) years and whenever changes are made that affect the potential risk level of operating the system. Ongoing Authorization (OA) will be discussed in later sections, and allows for ATOs that are greater than three years. "Operational" is generally defined as whenever an information system begins processing real or live data. An information system must be assessed and authorized in an Accreditation Decision Letter prior to passing the Key Decision Point 3 milestone in the development life cycle.

AOs may grant an Interim Authorization to Operate (IATO) for information systems that are undergoing development testing or are in a prototype phase of development. The AO may grant an IATO for a maximum period of six (6) months and may grant a single six (6) month extension. IATOs are not authorized for operational systems. IATOs are typically granted in the instance of a non-operational development information system testing with production data. In general, IATOs are not recognized within DHS.

The process for conducting a re-authorization is the same used to conduct the initial Security Authorization. The primary difference is that an initial Security Authorization should be started early in the System Engineering Life Cycle (SELC) process while re-authorization will usually begin four (4) to six (6) months before the current ATO expires. The four (4) to six (6) month timeframe assumes that resources are available to start the security authorization process. Additional lead time may be needed for contracting or otherwise obtaining resources needed to conduct the security authorization.

1.2 PURPOSE

The security authorization process applies the Risk Management Framework (RMF) from NIST Special Publication (SP) 800-37. This includes conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. This process helps ensure that managing information system-related security risks is consistent with the DHS mission/business objectives and overall risk strategy established by the department and components; integrates information security, including security controls, are integrated into the DHS enterprise architecture and SELC process; and supports consistent, well-informed security authorization decisions throughout the life-cycle of the information system.

The purpose of this document is to provide practical guidance for conducting a security authorization within DHS. Components may tailor this guide to meet their individual requirements as long as they remain consistent with this guide, NIST guidance, OMB guidance and directives, DHS security policies, guidance and directives, and all applicable laws, directives, policies, and directed actions.

1.3 SCOPE

All unclassified systems, including General Support Systems (GSSs) and Major Applications (MAs), in the DHS FISMA inventory must be assessed and authorized in accordance with the process identified in this guide. All sub-systems and minor applications must be documented in the security authorization package of an associated GSS or MA.

The process for assessing and accrediting National Security Systems (NSS) is outside the scope of this guide.

2.0 ROLES AND RESPONSIBILITIES

Within DHS guidelines, each Component, organization and system determines its own internal procedures for conducting a security authorization. In some cases, security authorizations are conducted by ISSOs. In other cases, a system may use contractors hired specifically to conduct the security authorization or Components may provide a dedicated security authorization group for use within the Component. The following sections list personnel who have a key role in the security authorization process and briefly describe their duties.

2.1 AUTHORIZING OFFICIAL (AO)

The Authorizing Official (AO) determines the degree of acceptable risk based on mission requirements, reviews the Security Authorization Package, and grants or denies ATO.

The DHS CIO serves as the AO for all Department-level enterprise systems or designates an AO in writing. The Component CIO serves as the AO for Component information systems or designates one in writing. The DHS Chief Financial Officer (CFO) serves as the AO for CFO Designated Systems managed at the DHS level. The Component CFO is the AO for only CFO Designated Systems managed by the Component.

2.2 CHIEF INFORMATION SECURITY OFFICER (CISO)/INFORMATION SYSTEM SECURITY MANAGER (ISSM)

The DHS Chief Information Security Officer (CISO) provides overall guidance for conducting a Security Authorization. The Component Chief Information Security Officer (CISO)/Information System Security Manager (ISSM) provides specific guidance for the Security Authorization Process within the Component and serves as the SCA unless someone else is designated.

2.3 DHS INVENTORY TEAM

The Federal Information Security Management Act (FISMA) requires developing, maintaining, and updating an inventory of information systems operated by the DHS or under its control. This inventory also includes an identification of the interconnections between each system and all other systems or networks, including those not operated by or under the control of the Department. The DHS Information Technology (IT) system inventory is also used to support information resources management; IT planning, budgeting, and acquisition; the monitoring, testing, and evaluation of information security controls; and the preparation of the index of major information systems required pursuant to the Freedom of Information Act (FOIA). The DHS Chief Information Security Officer (CISO), and subsequently the Inventory Management (IM) Team within OCISO, is responsible for ensuring Department-wide oversight and compliance with FISMA to include developing and maintaining a Department IT system inventory.

The DHS IM Team’s role consists of two primary functions: perform routine change management; and conduct the annual refresh process.

DHS Components are required to submit a Change Request form to the IM team any time the System Engineering Lifecycle (SELC) status or centrally managed data fields of an information system owned or operated by DHS changes. It is the IM team’s responsibility to process change requests and update the Information Assurance Compliance System (IACS), reporting system as needed. More information can be found in the DHS FISMA System Inventory Methodology.

The IM Team also conducts an annual review of all DHS information systems called the FISMA Inventory Annual Refresh. The Annual Refresh is an opportunity for Components to holistically review and update their inventory and for the ISO to clarify any discrepancies found through independent reviews. More information may be found in the FISMA Inventory Methodology guide.

2.4 SECURITY CONTROL ASSESSOR (SCA)

The Security Control Assessor (SCA) assesses the effectiveness of the security controls based on the documentation submitted in the Security Authorization Package and makes a recommendation to the AO regarding whether or not to authorize the system. The Security Authorization Team should coordinate closely with the SCA throughout the process to ensure they understand and meet DHS and Component requirements.

The Component CISO is normally the SCA when no other person has been officially designated.

The SCA tests the security controls documented in the Requirements Traceability Matrix (RTM). The RTM is created automatically in IACS, and the controls are tested to ensure they have been implemented properly and are operating as intended. The Security Assessment is usually conducted using the Security Assessment Plan developed by the Security Authorization Team. Members of the Security Assessment Team should not be on the Security Authorization Team to avoid conflict of interest but do not need to be independent for systems categorized as Low-Low-Low, confidentiality, integrity, and availability security categories, as long as test results are reviewed by an independent source to validate their completeness, consistency, and veracity. The AO decides the required level of independence based on the criticality and sensitivity of the system and the ultimate level of risk.

Figure 2 illustrates the information flow among various stakeholders needed to complete the Security Authorization process.

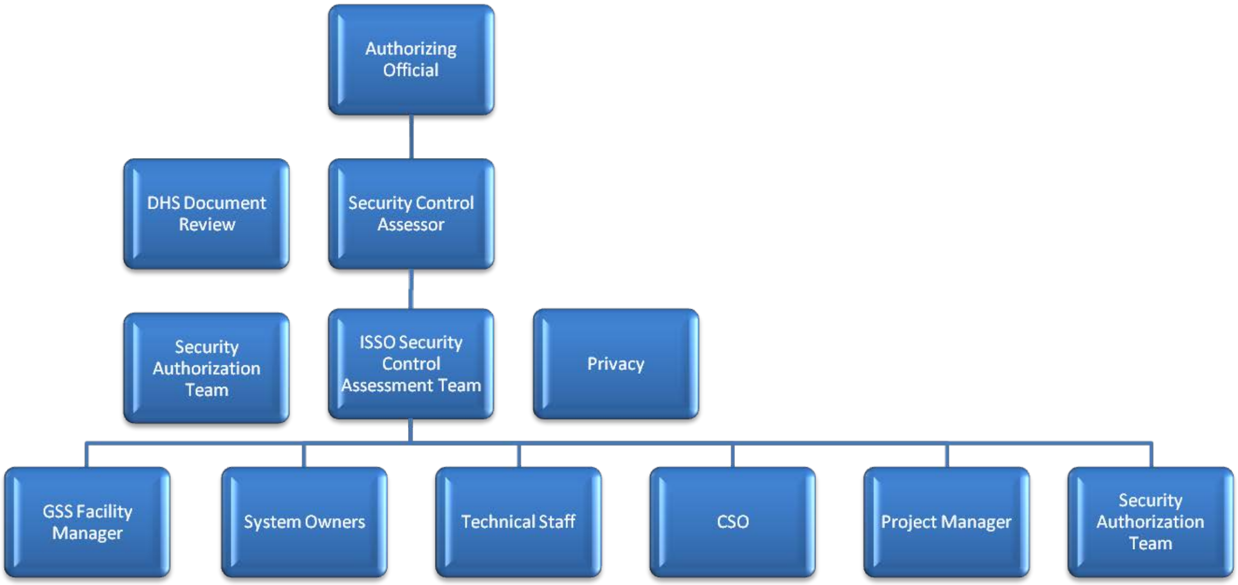
Authorizing Official
DHS Document Review
Security Control Assessor
Security Authorization Team
ISSO Security Control Assessment Team
Privacy
GSS Facility Manager
System Owners
Technical Staff
CSO
Project Manager
Security Authorization Team

Figure 2: The Security Control Assessor

2.5 SECURITY AUTHORIZATION TEAM

The security authorization team has primary responsibility for conducting security authorization activities. This includes collecting data, developing documents and preparing the Security Authorization Package (SAP) for the Security Control Assessor (SCA)/AO review. The security authorization team may also conduct the SAP depending on the need for separation of duties. The security authorization team needs access to the DHS security authorization Information Assurance Compliance System (IACS) tool.

Figure 1 illustrates the different stakeholders that must be engaged in order to conduct an efficient security authorization.

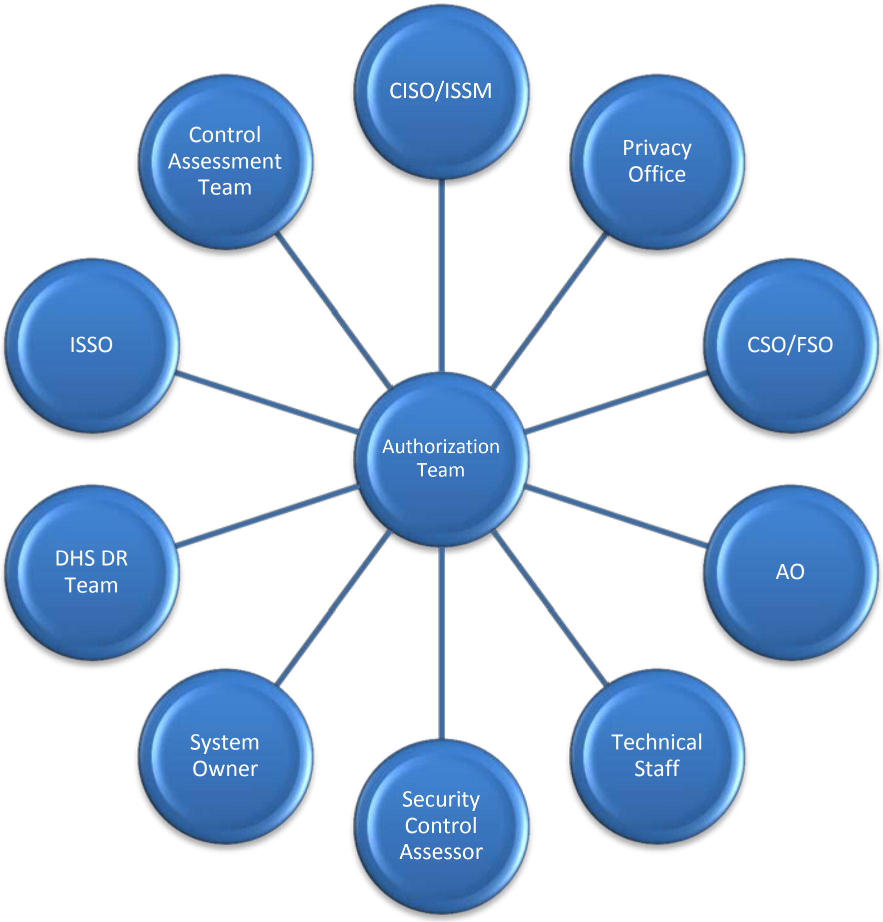

Figure 1: The Security Authorization Team Stakeholders

2.6 INFORMATION SYSTEM SECURITY OFFICER (ISSO)

Information System Security Officers (ISSOs) are not always directly responsible for conducting a Security Authorization but they need to monitor and oversee the process at a minimum. ISSOs need to be aware of the status and expiration of the current ATO and initiate action early enough to ensure the Security Authorization process is completed before the system becomes operational or the current ATO expires. This entails working closely with the System Owner or program manager to ensure resources are available to both conduct and to participate in the Security Authorization process. Regardless of how the process is implemented, the ISSO plays a leading role to ensure documents are created in IACS and submitted to the SCA for DHS validation. ISSOs should coordinate closely with the SCA and the AO before and during the Security Authorization process to ensure they are aware of requirements, processes and expectations.

2.7 SYSTEM OWNER

The System Owner must ensure that adequate resources are budgeted for and allocated to the Security Authorization process. The System Owner will also serve as a primary source of input during data collection activities and should review the package for accuracy before it is forwarded to the SCA/AO. The System Owner must also be involved in POA&M planning to help determine resource availability and schedule. System Owners are ultimately accountable for the security of their systems and should be directly involved in the Security Authorization process.

2.8 BUSINESS OWNER

The business owner may provide input needed for the system categorization and section one (1) of the Security Plan. The business owner may also provide resources for conducting the Security Authorization or remediating weaknesses.

2.9 PROGRAM MANAGER

The Program Manager may be a source of resources (e.g., if the Security Authorization process needs to be outsourced) and information input for areas where the System Owner is not knowledgeable (e.g., contracts).

2.10 TECHNICAL STAFF

A system's technical staff (e.g., system administrators, Data Base Administrators (DBAs), etc.) is the primary source of input for describing and implementing most technical controls identified in the Security Plan. They may also have input to the system categorization process depending on system technology (e.g., wireless) and configuration. The technical staff should participate in the SAP to provide input to the SAP team and oversee the actual testing.Chief Security officer (CSO)/Facility Security Officer (FSO)

The Chief Security Officer (CSO) and the Facility Security Officer (FSO) are often responsible for the implementation of some controls (e.g., physical access controls) and may provide input needed for personnel and physical controls for the system.

2.11 PRIVACY OFFICE

Senior Agency Officials for Privacy (SAOP) are responsible for the implementation of NIST SP 800-53 Appendix J. SAOPs will consult with other agency officials, including program mangers/information system owners, Authorizing Officials, Chief Information Officers, and Chief Information Security Officers in fulfilling this responsibility. However, the authority for selection and assessment of privacy controls ultimately rests with SAOPs.

For DHS, the Privacy Office selects and implements the privacy controls for each system. ISSOs and system owners are not part of this process and must not modify the privacy controls.

2.12 DHS DOCUMENT REVIEW TEAM (DR)

The DHS Document Review (DR) Team reviews and validates security authorization packages after they have been completed in IACS. Procedures for requesting a review can be found in the DHS Information Security Performance Plan and the DHS Document Review Methodology documentation.

3.0 RISK MANAGEMENT FRAMEWORK

The Risk Management Framework (RMF) provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The RMF operates primarily at the information system level; however, considerations of organizational risk must be taken into account when devising a risk management strategy. Communication between the organization and the system owner are also critical in maintaining a risk management strategy and ensuring events that impact the risk are accounted. The RMF steps include categorize, select, implement, assess, authorize, and monitor. More information can be found in the NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems".

3.1 CATEGORIZE

The security categorization is carried out by the system owner and the ISSO in cooperation with various organizational personnel. Information systems are categorized by the mission that the systems support.

PROJECT PERSONNEL

This task is for defining and documenting all the personnel who have responsibilities to assess the system or program.

ISSO DESIGNATION

All ISSOs must be designated in writing following the guidance in DHS MD 4300A Attachment N. ISSO letters define duties and responsibilities and are usually signed by the System Owner. ISSO letters must be updated whenever a change occurs. The designated ISSO should be consistently identified in three sources: the ISSO letter, the SSP and in IACS

SYSTEM USERS

This task is for identifying and adding users with responsibilities of the system or program in regards to operation, administration, maintenance and security. These are not individual users but rather categories of users (i.e., system administrators, patch managers, etc.). This allows minimum qualifications to users in any of these categories to be documented.

SYSTEM BOUNDARY

This task defines all computers and related equipment within a location(s), defined under the System Environment step, along with the internal and external connections (e.g., a router and all systems connected to its local-area ports). Graphical representations of the system boundary should be created.

PORTS PROTOCOLS & SERVICES

This task defines the routes by which the data flows through the system (e.g., flow of information between database servers and application servers; local network connections for backup or system mirroring; flow of routine e-mail traffic, etc.).

SYSTEM ENVIRONMENT

The System Environment task defines the environments or locations in which the system operates. Threat levels associated with each location/environment will be outlined. This information is published in the SSP and the Risk Assessment documentation.

E-AUTHENTICATION

OMB requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. Assurance levels also provide a basis for assessing Credential Service Providers (CSPs) on behalf of Federal agencies. This document will assist agencies in determining their e-government authentication needs. Agency business-process owners bear the primary responsibility to identify assurance levels and strategies for providing them. This responsibility extends to electronic authentication systems. This task defines the e-authentication level of the system. The determination of the e-authentication level is performed outside of the tool via the e-authentication workbook

SYSTEM DATA TYPES

This task is for categorizing system information types. An information type is a specific category of information defined by the DHS Business Reference Model (BRM).

SYSTEM SECURITY

The System Security task defines the information technology security parameters and the depth of testing that is to be performed on the components of the system being authorized based upon the FIPS 199 security categorization. This information is used to calculate the system’s protection level, which determines the type and intensity of the testing that will be performed.

3.2 SELECT

Once the FIPS 199 categorization is performed for each security objective, the DHS baseline of controls is applied. DHS contains both NIST security controls and DHS 4300A requirements as enhancements to NIST security controls. Although this baseline provides a minimum set of controls, the component, AO, system owner, and ISSO may determine more controls are necessary to mitigate the risk to an acceptable level. Other considerations should also be taken into account when selecting controls. For example, DHS CFO designated systems affect the risk of DHS and have specific controls that must be evaluated, tested, and documented annually to reduce the overall risk to an acceptable level.

During the security control selection process organizations may begin planning for the continuous monitoring process by developing a monitoring strategy. The strategy can include, for example, monitoring criteria such as the volatility of specific security controls and the appropriate frequency of monitoring specific controls. Typically, the component will have a continuous monitoring program to provide overall guidance, requirements and monitoring of certain controls. The system owner and ISSO can leverage and supplement this component program with a strategy that is tailored to the system to provide coverage to any area the component continuous monitoring program may not be able to cover.

The selected security controls are documented in a system security plan (SP). The security plan contains an overview of the security requirements for the information system in sufficient detail to determine that the security controls selected would meet those requirements. The security plan, in addition to the list of security controls to be implemented, describes the intended application of each control in the context of the information system with sufficient detail to enable a compliant implementation of the control.

Privacy controls are under the authority of and determined by the Privacy Office. ISSOs and system owners are not to address these controls.

REQUIREMENTS QUESTIONNAIRE

This task contains questions about the system being assessed to determine if requirements are applicable or not. For the questions listed, answer them by selecting Yes or No and then save. The results of this questionnaire will help determine the requirement's applicability as shown on the System Security Requirements page.

ORGANIZATIONALLY DEFINED REQUIREMENTS

Security controls and control enhancements containing embedded parameters (i.e., assignment and selection statements) give organizations the flexibility to define certain portions of controls and enhancements to support specific organizational requirements. After the initial application of scoping considerations and the selection of compensating controls, organizations review the security controls and control enhancements for assignment/selection statements and determine appropriate organization-defined values for the identified parameters.

This step defines the requirement assignment questions that are used to collect specific information that vary from organization to organization. All of the questions on this page are based on DHS guidance (e.g., 3 attempts, 90 days). The answers are added automatically to the associated requirement, identified by the paragraph number in the brackets at the end of the question. The answers replace existing text, such as [Assignment: organization-defined time period].

3.3 IMPLEMENT

Security control implementation is described, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs). Security control documentation describes how system-specific, hybrid, and common controls are implemented. The documentation formalizes plans and expectations regarding the overall functionality of the information system. The functional description of the security control implementation includes planned inputs, expected behavior, and expected outputs where appropriate, typically for those technical controls that are employed in the hardware, software, or firmware components of the information system. Documentation of security control implementation allows for traceability of decisions prior to and after deployment of the information system. The documentation also addresses platform dependencies and includes any additional information necessary to describe how the security capability required by the security control is achieved at the level of detail sufficient to support control assessment.

After the security controls are documented in the SP, they are implemented in accordance with their descriptions in the SP. Best practices are used when implementing security controls. These include system and software engineering methodologies, security engineering principles, and secure coding techniques. Risk assessments may help inform decisions regarding the cost, benefit, and risk trade-offs in using one type of technology versus another for control implementation. In addition, the system owner and ISSO ensure mandatory configuration settings are established and implemented on information technology products in accordance with federal, DHS, and component policies. When available, the system owner and ISSO should consider the use of information technology products that have been tested, evaluated, or validated by approved, independent, third-party assessors. The security plan is updated as the controls are implemented to ensure the documented control implementation is consistent with the actual implementation.

IMPLEMENT SECURITY CONTROLS

Once security controls are selected, it is necessary to implement them for the information system. This formalizes plans and expectations regarding the overall security of the information system. The description of the security control implementation includes planned inputs, expected behavior, and expected outputs where appropriate. At a minimum, the security controls must address the, what, where, who and how often questions outlined in the Document Review Methodology.

EQUIPMENT GROUPS

Equipment groups should be defined for each location within the project. It is important to define the equipment groups, before importing the equipment, to both provide a process for grouping the equipment inventory during the import and for easily categorizing the components of the information system. The ISSO can use the default set of groups provided here or simply add/modify the equipment groups to best fit the individual system environment.

EQUIPMENT INVENTORY

Define specific details of computers, servers, printers that exist within the boundary of the information system. This step allows either manual entry of equipment or import an inventory list directly into the project, such as a Nessus scan file. Each individual piece of equipment can be characterized in detail, including hardware description, network address, operating system, information on installed software applications, and indication if the equipment will be tested. This information is used to build the appropriate equipment tests defined in the test plan for the system.

MANAGE SOFTWARE

Once equipment is identified for the project, all the installed software will be displayed here along with the associated equipment count. ISSOs will review the list of software applications and make any necessary modifications. Since software applications are directly linked to equipment inventory and test procedures, this ensures the appropriate test procedures are pulled on the Test Plan & Results step.

SECURITY PLAN

System security plans are living documents that require periodic review, modification, and plans of action and milestones for implementing security controls. Procedures should be in place outlining who reviews the plans, keeps the plan current, and follows up on planned security controls. In addition, procedures should require that system security plans be developed and reviewed prior to proceeding with the security certification and accreditation process for the system.Security Plan Extensible

CONTINGENCY PLAN AND TEST

The intent of a contingency plan, as described by Section 3.5.2 of the *DHS 4300A Sensitive Systems Handbook,* is to ensure the availability of critical information systems under all circumstances. A Contingency Plan provides for capability to respond to emergencies, to recover from them, and to resume normal operations, possibly at an alternate location, in the event of emergency, system failure, or disaster.

Specific control requirements for emergency situations, and level of effort expended, are determined based on the information system's security categorization. The level of resources for the Contingency Plan is based on the security categorization for the availability security objective:

- For systems with a **low impact for availability**, the system owner can determine the Contingency Plan format and content that is appropriate for the system and its environment. The Contingency Plan generated in the Information Assurance Compliance System (IACS) automated Security Authorization tool can also be used.
- For systems with a **moderate impact level for availability**, the default Contingency Plan template in IACS should be used.
- Systems with a **high impact level for availability** should develop a rigorous Contingency Plan. The template to be used for such a plan is provided in this attachment (see below). It can also be found in IACS. The high impact plan can be received in IACS when creating a package, by answering "Yes" to additional documents in the questionnaire.

CONFIGURATION MANAGEMENT PLAN

The Configuration Management Plan ensures that configuration and control changes to the system are monitored, evaluated, and impacts are assessed prior to implementation. This step is divided into several sections which correspond to sections in the configuration management plan. Configuration Management Plan Extensible

3.4 ASSESS

Conducting security control assessments in parallel with the development/acquisition and implementation phases of the life cycle permits the identification of weaknesses and deficiencies early and provides the most cost-effective method for initiating corrective actions. Issues found during these assessments can be referred to authorizing officials for early resolution, as appropriate. The results of security control assessments carried out during system development and implementation can also be used (consistent with reuse criteria) during the security authorization process to avoid system fielding delays or costly repetition of assessments.

SECURITY ASSESSMENT PLAN

The security assessment plan provides the objectives for the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures. The assessment plan reflects the type of assessment the organization is conducting (e.g., developmental testing and evaluation, independent verification and validation, assessments supporting security authorizations or reauthorizations, audits, continuous monitoring, assessments subsequent to remediation actions).

SECURITY ASSESSMENT

Security control assessments determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Security control assessments occur as early as practicable in the system development life cycle, preferably during the development phase of the information system.

SELF-ASSESSMENT

The self-assessment is conducted as an initial test by the host to get a basic understanding of the system's security posture. When self-assessment is complete, security assessment is conducted.

TEST PLAN & RESULTS

The project test matrix provides a detailed overview of the requirements and associated test procedures included in the test plan for the information system. This saves time and effort required to manually search through the test plan for this information. It provides a detailed summary of applicable test procedures and an explanation of those tests that are not applicable due to equipment type, equipment scope, etc.

RISK ANALYSIS

Risk Analysis is the last task in the Assess phase, where the controls put in place in the Implementation phase are assessed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. At this point, the self-assessment and security assessment have been completed. The final certification analysis will be conducted and documentation will be updated in preparation for the next task. The Analyze Risk Elements step presents a list of information system's risk elements and provides the tools and information required to review and analyze them. A risk element is an item from a failed test or a user-defined item that could potentially impact the security of the system based upon threats and vulnerabilities to the information system.

RISK ASSESSMENT (RA)

This step documents the results and analysis of the tests performed on the system. All of the information used for this report is primarily captured on the analyze risk elements step.

SECURITY ASSESSMENT REPORT (SAR)

The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the security assessment report. The security assessment report is one of the key documents in the security authorization package developed for authorizing officials. The security assessment report includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the SCA findings. The security assessment report is an important factor in an authorizing official's determination of risk to organizational operations and assets, individuals, other organizations, and the Nation.

SYSTEM RISK LEVEL

This step provides the ability to review, discuss and adjust the risk level assigned to the system as a whole as determined by the Analyze Risk Element step. The SCA will adjust the risk level if necessary.

3.5 AUTHORIZE

Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

The plan of action and milestones, prepared for the authorizing official by the information system owner or the common control provider, is one of three key documents in the security authorization package and describes the specific tasks that are planned: (i) to correct any weaknesses or deficiencies in the security controls noted during the assessment; and (ii) to address the residual vulnerabilities in the information system. The plan of action and milestones identifies: (i) the tasks to be accomplished with a recommendation for completion either before or after information system implementation; (ii) the resources required to accomplish the tasks; (iii) any milestones in meeting the tasks; and (iv) the scheduled completion dates for the milestones. The plan of action and milestones is used by the authorizing official to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment. All security weaknesses and deficiencies identified during the security control assessment are documented in the security assessment report to maintain an effective audit trail. Organizations develop specific plans of action and milestones based on the results of the security control assessment and in accordance with applicable laws, Executive Orders, directives, policies, standards, guidance, or regulations. Plan of action and milestones entries are not required when weaknesses or deficiencies are remediated during the assessment or prior to the submission of the authorization package to the authorizing official.

The authorize phase of the risk management framework (RMF) is where the AO makes a decision whether or not to authorize the system for operation based on the security plan, security assessment report, and the plan of actions and milestones (POA&M). This provides the AO, at a minimum, the necessary information about risk impact.

POA&M

A Plan of Action and Milestones (POA&M) is mandated by the Federal Information Systems Management Act of 2002 (FISMA) as a corrective action plan for tracking and planning the resolution of information security weaknesses. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. The 4300A Attachment H “Process Guide for Plan of Action and Milestones,” constitutes the core process for remediating control deficiencies in sensitive Department of Homeland Security (DHS) information systems.

COMPONENT DOCUMENT REVIEW

The purpose of the Component document review (DR) is to implement a rigorous set of quality standards across the Component Security Authorization (SA) packages to ensure that applicable DHS and NIST controls have been properly documented.

ATO DECISION

In the ATO Decision task, the Authorizing Official (AO) will review the accreditation package and make the decision to grant or deny authorization to operate (ATO). The Project Accreditation (with history) is used to indicate the authorization type granted to projects based on the results of the assessment effort, as well as to maintain a project's authorization history. The ATO Letter provides authorization to operate information systems or to use security controls inherited by those systems.

DHS DOCUMENT REVIEW

The goal of document review (DR) is to implement a rigorous set of quality standards across all DHS Security Authorization (SA) packages to ensure that applicable DHS and NIST controls have been properly documented. Where applicable, the DR team will enforce the creation of mitigation plans for control requirements that have not been met

3.6 MONITOR

Information systems are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and operate. A disciplined and structured approach to managing, controlling, and documenting changes to an information system or its environment of operation is an essential element of an effective security control monitoring program. Strict configuration management and control processes are established by the organization to support such monitoring activities. It is important to record any relevant information about specific changes to hardware, software, or firmware such as version or release numbers, descriptions of new or modified features/capabilities, and security implementation guidance. It is also important to record any changes to the environment of operation for the information system (e.g., modifications to hosting networks and facilities, mission/business use of the system, threats), or changes to the organizational risk management strategy. The information system owner and common control provider use this information in assessing the potential security impact of the changes. Documenting proposed or actual changes to an information system or its environment of operation and subsequently assessing the potential impact those changes may have on the security state of the system or the organization is an important aspect of security control monitoring and maintaining the security authorization over time. Information system changes are generally not undertaken prior to assessing the security impact of such changes.

4.0 ONGOING AUTHORIZATION

As stated in NIST 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, "initial system authorization is based on evidence available at one point in time, but systems and environments of operation change." To address the needs of constantly changing environments, DHS is implementing OA, which involves shifting from periodic to ongoing assessments and facilitates a continual state of awareness.

DHS implements OA in **three layers**, which collectively ensure constant control assurance.

- Layer 1: Common and Inherited Controls and Reciprocity
- Layer 2: Continuous Monitoring
- Layer 3: Event-Driven Monitoring

Event-Driven Monitoring (Layer 3) involves evaluating and testing controls when security events or "triggers" occur that may have an impact on the system's security status. Following an event, a review is conducted to determine the impact on the status of controls and risk to the system. Some key **process highlights** include the following:

- An Operational Risk Management Board (ORMB), composed of various subject matter experts, evaluates security triggers and makes risk-based recommendations.
- Following ORMB review, the CISO prepares a formal recommendation to the Authorization Official (AO) about whether or not to maintain the authorization.

Security triggers are to be reported in the Component's Trigger Accountability Log (TRAL) and provided to DHS on a monthly basis.

To qualify for OA, the following **prerequisites** must be met (see section 1.6 for more detail):

- The system must have a valid ATO.
- The information system must have a Control Allocation Table (CAT).
- The Component should have a Common Control Catalog in place.
- The Component must have a robust Continuous Monitoring program.
- The Component must assign an OA Manager.
- The Component must establish an ORMB.
- The Component must offer an OA training program.

The Component must accept and sign the DHS OA Memorandum of Agreement (MOA).

For more information about ongoing authorization, please refer to the Ongoing Authorization Methodology guide.

5.0 CLOUD AND FEDRAMP AUTHORIZATIONS

Cloud computing relies on restricting sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. Cloud computing provides scalable information technology (IT) capabilities that are offered as a service over the Internet to many users at one time. Multiple agencies can share pooled IT resources, such as an email service, that reduce costs and improve efficiency.

Cloud computing, or in simpler shorthand just "the cloud," also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental impact as well since less power, air conditioning, rack-space, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.

Clouds are categorized by their deployment models. The deployment model is based on the organizational structure, provisioning location, security considerations, and budget. The cloud deployment models are public, private, hybrid, and community clouds.

A "public" cloud infrastructure is available to the general public and is owned by a third party cloud service provider (CSP). In a public cloud, an agency dynamically provisions computing resources over the Internet from a CSP who shares its resources with other organizations. Similar to that of an electric utility billing system, the CSP bills the agency for its share of resources.

This can be the most cost effective deployment model for agencies as it gives them the flexibility to procure only the computing resources they need and delivers all services with consistent availability, resiliency, security, and manageability. Nevertheless, to benefit from a public cloud, an agency must accept the reduced control and monitoring over the CSP's governance and security.

A "private" cloud infrastructure is operated solely for a single organization or agency: the CSP dedicates specific cloud services to that agency and no other clients. The agency specifies, architects, and controls a pool of computing resources that the CSP delivers as a standardized set of services. A common reason for agencies to procure private clouds is their ability to enforce their own data security standards and controls.

An agency will typically host a private cloud on premises, connect to it through private network links, and only share its resources within the agency. Because resources are not pooled across multiple unaffiliated organizations, an agency will pay for all of the cloud's capacity. Nevertheless, the agency's Chief Information Officer (CIO) can provide these resources as services on-demand to organizations and programs within the agency and charge them accordingly.

A "hybrid" cloud comprises two or more clouds (private, community, or public) with a mix of both internally and externally hosted services.

Agencies will likely not limit themselves to one cloud deployment but will rather incorporate different and overlapping cloud services to meet their unique requirements. Hybrid deployment models are complex and require careful planning to execute and manage especially when communication between two different cloud deployments is necessary.

The Federal Risk and Authorization Management Program (FedRAMP) provides a cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies:

- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels;
- A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by Cloud Service Providers (CSPs);
- Authorization packages of cloud services reviewed by a Joint Authorization Board (JAB) consisting of security experts from the Department of Homeland Security (DHS), Department of Defense (DOD), and General Services Administration (GSA);
- Standardized contract language to help Executive departments and agencies integrate FedRAMP requirements and best practices into acquisition; and
- A repository of authorization packages for cloud services that can be leveraged government-wide.

FedRAMP processes are designed to assist agencies in meeting FISMA requirements for cloud systems and addresses complexities of cloud systems that create unique challenges for complying with FISMA.

There are three paths to achieving FedRAMP compliance:

1. A Cloud Service Provider (CSP) can submit the appropriate documentation to the FedRAMP PMO and to the JAB which may grant a Provisional Authorization to Operate (P-ATO)
2. A Cloud Service Provider can submit the appropriate documentation to the FedRAMP PMO and to an agency which may grant an agency “Authorization to Operate” (ATO). Using FedRAMP mechanisms, other agencies can then “leverage” this ATO for use in their agency, decreasing the time for approvals.
3. A Cloud Service Provider can use the “CSP supplied” path by submitting the appropriate documentation to the FedRAMP PMO. While this does not grant the CSP a P-ATO or an agency ATO, it decreases the time for approvals because documentation and testing (by a Third Party Assessment Organization or 3PAO) are complete and available for agency review.

There are three paths for security packages to make their way into the FedRAMP repository. Once a security package is listed in the FedRAMP repository, federal agencies then have the opportunity to review the packages to determine if they would like to use the system described in the package. Some of the packages listed in the repository may already be approved as being FedRAMP compliant while other packages are candidates for approval.

FedRAMP package categories are CSP, Agency ATO, and JAB P-ATO. It is possible for a package to move from one level to another. Categories do not necessarily represent the strength of the security controls for the represented cloud system. The biggest difference between the three categories is the level of security package review. DHS private clouds must go through both the DHS security authorization process and submission to FedRAMP. DHS private clouds are categorized as Agency ATO for FedRAMP purposes.

CSPs may supply a security package to the FedRAMP secure repository for DHS use. In this case, a CSP decides to work independently instead of through the JAB or through a Federal agency. In this category, a CSP will complete the FedRAMP SAF independently and will not have an authorization at the completion, but will have a FedRAMP-compliant package available for leveraging.

For CSP -supplied packages, CSPs must contract with an accredited 3PAO to independently verify and validate their security implementations and their security assessment package.

Once a CSP completes their security authorization package, the CSP must inform the FedRAMP PMO by sending an email to info@FedRAMP.gov. The PMO then instructs the CSP how to submit the package for PMO review. After reviewing the package to ensure it meets all of the FedRAMP requirements, the FedRAMP PMO will publish the package in the secure repository for other agencies to leverage.

If an Agency decides to issue an ATO to a CSP-supplied package, the status of the package will be changed in the secure repository to indicate that it has evolved to a FedRAMP Agency ATO Package.

Once an agency reviewer determines which package to review, the next step is to download the FedRAMP Package Access Request Form from www.fedramp.gov and fill in all of the requisite fields. The form needs to be reviewed and signed internally at the reviewer's agency by the reviewer's CISO, before submitting it to the FedRAMP PMO. In the event that the agency has more than one CISO, the signature should come from the CISO that is closest in the line of reporting to the reviewer.

Once the authority within the requesting agency signs the form, prospective package reviewers must scan the signed access request form and email it to info@fedramp.gov. The form will be reviewed for correctness and completeness by the FedRAMP PMO. All information on the form is subject to verification.

There are certain limitations that government contractors face in reviewing FedRAMP security packages. Security packages contain intellectual property of each respective CSP. If the prospective package reviewer is a government contractor, the FedRAMP PMO will contact the CSP system owner to obtain their approval.

The prospective package reviewer will be notified and provided access instructions when the request is approved or denied. A new FedRAMP Package Access Request Form must be filled

In accordance with DHS 4300A policy, all security authorizations are conducted and recorded in the Information Assurance and Compliance System (IACS). Refer to Appendix A for more information on IACS and how to obtain an account.

FedRAMP systems are implemented, assessed, and monitored in IACS like any normal system. IACS uses control inheritance to leverage a FedRAMP system. In order to use a FedRAMP system, the Common Control Team (CCT) must be informed. To submit a request to the CCT, please contact the DHS Information Security Customer Service Center (Infosec Helpdesk). After obtaining access, leveraging a FedRAMP system is similar to inheriting controls from a non-FedRAMP system.

To submit a system to FedRAMP, contact the Infosec Helpdesk to start the process of converting a system to a FedRAMP system.

All systems must go through the DHS security authorization process and have an ATO granted whether they are going to FedRAMP or not. For FedRAMP systems, there are three types of security authorizations, Agency ATO, Agency 3PAO, or JAB P-ATO.

Agency ATO is not different than the normal DHS security authorization process with the exceptions of satisfying FedRAMP controls and registering the system with FedRAMP. This type of authorization is intended for internal DHS component use.

Agency 3PAO authorizations go through a third party independent assessor. The system must satisfy FedRAMP controls and be registered with FedRAMP. This type of authorization is intended for internal DHS use but is shared among components.

The FedRAMP JAB P-ATO is a system which goes through the DHS security authorization process, is assessed by a 3PAO, is submitted to FedRAMP, is reviewed by the JAB, and granted an ATO by FedRAMP for use within the Federal government. This type of authorization is intended for systems that provide a service to the entire federal government and must go through a rigorous security authorization.

A system leveraging responsibilities is known as a tenant. Tenants are still accountable for the security of their system even if the CSP is providing controls and services. The tenant has the responsibility to address any security gaps that may arise between what the CSP is providing and the tenant is consuming.

Within the FedRAMP Security Assessment Framework, once an authorization has been granted, the CSP's security posture is monitored according to the assessment and authorization process. Monitoring security controls is part of the overall risk management framework for information security and is a requirement for CSPs to maintain a security authorization that meets the FedRAMP requirements.

Traditionally, this process has been referred to as "Continuous Monitoring" as noted in *NIST SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations*. Other NIST documents such as NIST SP 800-37, Revision 1 refer to "ongoing assessment of security controls". It is important to note that both the terms "Continuous Monitoring" and "Ongoing Security Assessments" mean essentially the same thing and should be interpreted as such.

As described in the FedRAMP requirements, CSPs must provide monthly reports of all vulnerability scanning to authorizing officials for review and tracking these vulnerabilities within the POA&Ms. These deliverables are really a subset of the evidence required at time of authorization. In this vein, the analysis of these scan results should be performed in the same manner they were for time of authorization. In particular, this means:

- All scan findings must be documented (including low findings).
- Each unique vulnerability is tracked as an individual POA&M item.
- Deviation requests must be submitted for any requested changes to scan findings (e.g. risk adjustments, false positives, and operational requirements).

On a monthly basis, Authorizing Officials will be monitoring these deliverables to ensure that the CSP maintains an appropriate risk posture – which typically means the risk posture stays at the level of authorization or improves. As a part of any authorization letter, CSPs are required to maintain a continuous monitoring program. CSPs should understand that this means their continuous monitoring deliverables and associated view of risk posture means that this analysis on a monthly basis leads to a continuous authorization decision every month by Authorizing Officials.

In an effort to aid agencies in their analysis and help CSPs understand how agency authorizing officials will analyze the continuous monitoring deliverables, the following are some details on how the FedRAMP PMO and JAB analyze continuous monitoring deliverables for those CSPs who achieve a P-ATO.

Some notes on the analysis of reporting within continuous monitoring for JAB P-ATOs:

- Summary information is requested from CSPs in order to provide easier analysis of the continuous monitoring reporting (the reporting format is provided below).
- Verifying what CSPs provide and their analysis is imperative to ensure that the risk posture is accurately depicted in this summary information.

- Trending data is imperative to understand the overall effectiveness of a CSPs continuous monitoring program.
- Late POA&Ms and risk are of high importance to the JAB. This details an inability of vendors to meet the FedRAMP requirements and identifies key risks that agencies should be aware of. Also, a repeated history of late POA&Ms is a key indicator of an ineffective continuous monitoring program and usually also indicates misaligned business processes and operations within a CSP.
- It is normal to have deviation requests and unique items for each vendor that must be analyzed on a system to system basis. Some specifics on how the JAB handles these unique items:
    - Date adjustments are not treated as deviation requests, as this does not change the fact that a POA&M is late for remediation within the required timeframes.
    - CSPs many times buy products or services and incorporates these in to their cloud environment to deliver their services. Many times risks can be related to these products and services and these risks are considered "vendor dependent." Risks are only considered vendor dependencies when remediating vulnerabilities within a product or service is not allowed by the vendor (e.g. it would void the warranty).
        - All vendor dependencies at a high risk level must be mitigated to a moderate through compensating controls within 30 days.
        - Vendor dependencies at the low and moderate level require CSPs to be in contact with their vendors at a minimum of a monthly basis to ensure there are no updates that would remediate the known vulnerabilities.
        - If a CSP contacts their vendors and provides evidence with their monthly deliverables of this contact regarding any fixes to the open vulnerabilities, then a vendor dependency is not considered a late POA&M.

Operational requirements exist only for vulnerabilities where the ability to remediate them does not exist or remediating vulnerabilities is not supported if the vulnerability is vendor dependent.

APPENDIX A: REFERENCES

- DHS Sensitive Systems Policy Directive 4300A
- DHS 4300A Sensitive Systems Handbook
- DHS Ongoing Authorization Methodology
- Attachments to DHS 4300A, particularly:
    - Attachment B, "*Waivers and Exceptions Request Form*"
    - Attachment C, "*Information Systems Security Officer (ISSO) Designation Letter"*
    - Attachment D, "*Type Accreditation*"
    - Attachment F, "*Incident Response and Reporting*"
    - Attachment G, "*Rules of Behavior*"
    - Attachment H, "*Plan of Action and Milestones (POA&M) Process Guide*"
    - Attachment K, "*IT Contingency Plan Template"*
    - Attachment N, "*Preparation of Interconnection Security Agreements*"
- NIST SP 800-53, "*Recommended Security Controls for Federal Information Systems and Organizations*"
- DHS CISO NIST SP 800-53 Security Controls tri-fold
- DHS FISMA System Inventory Methodology
- DHS Information Security Performance Plan
- DHS Document Review Methodology
- Document Review Checklists
- Security Authorization Document Templates
- FIPS-199 Workbook and Instructions
- Privacy Threshold Analysis (PTA) Template

Additional references that may be useful when conducting a Security Authorization include:

- Component specific guidance
- DHS Information System Security Officer (ISSO) Guide
- Telos Exacta User Guide and In-application Help
- Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
- Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publications (SPs) in the 800 series, but especially:
    - SP 800-18, "*Guide for Developing Security Plans for Federal Information Systems*"
    - SP 800-30, " *Guide for Conducting Risk Assessments*"

- SP 800-34, "*Contingency Planning Guide for Information Technology Systems*"
- SP 800-37, "*Guide for Applying the Risk Management Framework to Federal Information Systems*"
- SP 800-39, "*Managing Information Security Risk: Organization, Mission, and Information System View*"
- SP 800-53A, "*Guide for Assessing the Security Controls in Federal Information Systems*"
- SP 800-60, "*Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*"