NIST Special Publication 800-26
Revision 1

Guide for Information Security Program Assessments and System Reporting Form

Marianne Swanson
Joan Hash
Mark Wilson
Richard Kissel

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

INFORMATION SECURITY

INITIAL PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2005

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

U.S. Department of Commerce
Carlos M.Gutierrez, Secretary

Technology Administration
Michelle O'Neill, Acting Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William A. Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov — Phone: (202) 512-1800 — Fax: (202) 512-2250
Mail: Stop SSOP, Washington, DC 20402-0001

Acknowledgments

The authors wish to thank their colleagues who reviewed the draft of this document and contributed to its development. A special note of thanks also goes to Elizabeth Lennon for her technical editing.

Table of Contents

1. Introduction

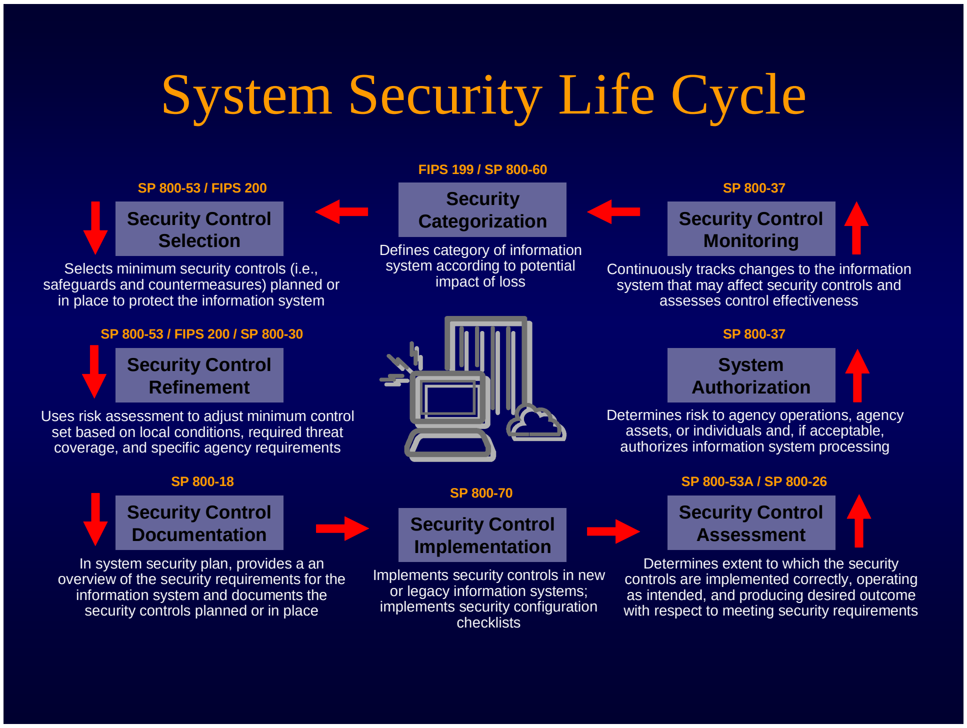
An assessment conducted on an agency-wide information security program, on an information system (major application or general support system), or multiple assessments conducted for a group of interconnected systems (internal or external to the agency) is one method used to measure information security assurance. Information security assurance is the degree of confidence one has that the managerial, technical, and operational security measures work together to form and maintain a viable information security program, and work as intended to protect a system and the information it processes. Adequate security of information system assets is a fundamental management responsibility. Consistent with the Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) policy, each agency must implement and maintain an information security program to adequately secure its information and system assets. Agency information security programs must: 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and 2) protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

Agencies must plan for security, ensure that the appropriate officials are assigned security responsibility and trained accordingly, review security controls, and authorize system processing prior to operations and periodically thereafter. These management responsibilities presume that responsible agency officials understand the risks and other factors that could negatively impact their mission goals. Moreover, these officials must understand the current status of their information security program and system-level security controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

An assessment is one method agency officials can employ to help determine the current status of their information systems and agency-wide information security program. Ideally, assessments of selected security controls on an ongoing basis should be conducted to systematically identify programmatic weaknesses and where necessary, establish targets for continuing improvement. This document provides a standardized form for reporting the results of system-level assessments and a method for evaluating the effectiveness of an agency information security program. Additionally, the document provides guidance on utilizing the results of the information security program and system assessments to ascertain the status of the agency-wide information security program.

1.1 System and Program-Level Assessments

Assessing the security of an information system and of an agency's information security program consists of two distinct tasks: 1) standard reporting of assessments conducted on an information system or a group of interconnected information systems; and 2) completion of an agency-wide security program-level questionnaire. In order to complete these tasks, an information security program must be established within the agency that supports the information system security life cycle. As noted in Figure 1 below, key life cycle activities, starting with Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems,*[1] and continuing through documenting an information system security plan should be completed before an information system can be assessed. The agency-wide information security program should also have documented policy and procedures in place that meet the criteria described in the Federal IT Security Assessment Framework.[2]



System Security Life Cycle

SP 800-53 / FIPS 200
Security Control Selection
Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

FIPS 199 / SP 800-60
Security Categorization
Defines category of information system according to potential impact of loss

SP 800-37
Security Control Monitoring
Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

SP 800-53 / FIPS 200 / SP 800-30
Security Control Refinement
Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements

SP 800-37
System Authorization
Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-18
Security Control Documentation
In system security plan, provides a an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70
Security Control Implementation
Implements security controls in new or legacy information systems; implements security configuration checklists

SP 800-53A / SP 800-26
Security Control Assessment
Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

Figure 1. System Security Life Cycle

1.1.1 System-Level Assessments

An agency must meet the minimum security requirements in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* by selecting the appropriate security controls and assurance requirements as described in NIST Special Publication (SP) 800-53, *Minimum Security Controls for Federal Information Systems*. System-level assessments are conducted by examining, reviewing, and testing the implementation of the appropriate security control baseline contained in NIST SP 800-53. The procedures for assessing the minimum security controls are contained in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.[3]

[1] See Section 2.1 System Inventory and FIPS 199 Categorization for a description of the FIPS 199 categorization process.

[2] The Federal IT Security Assessment Framework issued by the Federal Chief Information Officer (CIO) Council in November 2000 provides a method that agencies can use to routinely evaluate the status of their information security program. The document established the groundwork for standardizing on five levels of security effectiveness and measurements that agencies could use to determine which of the five levels are met. By utilizing the Framework levels, an agency can prioritize agency efforts as well as use the document over time to evaluate progress. The NIST Assessment Guide builds on the Framework by categorizing evaluation results in the same manner as the Framework.

[3] The first draft of NIST SP 800-53A was published summer 2005.

Since the above two NIST special publications provide the security controls and the assessment criteria, respectively, this guide points to the documents for reference. The System Reporting Form (Appendix A) is used to document the results of assessing each control listed in NIST SP 800-53. The reporting form contains the NIST SP 800-53 control name, number, and several other fields related to security controls that are explained later in this document. The assessment criteria contained in NIST SP 800-53A should be completed so that the results of the assessment are reported in a format that identifies for each control which of the five levels specified in the Federal IT Security Assessment Framework has been achieved by the system. It should be noted that an agency might have additional laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability. If the specific requirements require additional security controls, the security controls should be documented in the system security plan and added to the system-level reporting form.

The completed form may be used to identify the status of security controls for a system, an interconnected group of systems, or when combining many system-level assessments, the status of the agency's security program can be partially obtained. These systems include information, individual systems (e.g., major applications or general support systems), or a logically related group of systems that support operational programs (e.g., Air Traffic Control, Medicare, Student Aid). The reporting form should be provided to the system owner, system security officer, or the independent assessor who is evaluating the system or systems. Assessing all security controls and all interconnected system dependencies, reporting in a standardized format, and analyzing the results provides a metric of the information security conditions of an agency.

1.1.2 Information Security Program Assessment

To assist agencies in meeting their annual FISMA reporting requirements, the Information Security Program Assessment Questionnaire (Appendix B) provides questions on many of the areas typically required for inclusion in agency reports. The first part of the questionnaire asks for the cumulative results of the system-level assessments. The second part contains agency-wide program-level questions that are not found in NIST SP 800-53 and/or the system-level assessments. The questionnaire can be customized with agency-specific, program-related questions and can be completed by the Chief Information Officer (CIO), Senior Agency Information Security Officer, or an independent assessor who is evaluating the agency information security program.

1.2 Roles and Responsibilities

Agencies should develop policy on the system and agency-wide program assessment process. Procedures should be in place outlining who performs assessments and when they should be performed. In addition, procedures are needed describing how assessment results are to be collected, compiled, analyzed, and used to meet OMB and other data calls.[4] Information security program management includes many duties; the roles and

[4] Departments may request periodic assessment results from their subordinate organizational units.

responsibilities in this section are specific to system and agency-wide program security assessments.

Chief Information Officer
The Chief Information Officer (CIO)[5] is the agency official responsible for developing and maintaining an agency-wide information security program and has the following responsibilities for system and program security assessments:

- Designates a senior agency information security officer (SAISO) who shall carry out the CIO's responsibilities for system and program security assessments,

- Develops and maintains information security policies, procedures, and control techniques to address system and program security assessments,

- Manages the identification, implementation, and assessment of common security controls,

- Ensures that personnel with significant responsibilities for system and program security assessments are trained, and

- Assists senior agency officials with their responsibilities for system and program security assessments.

Information System Owners
The *information system owner*[6] is an agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The information system owner has the following responsibilities related to system assessments:

- Incorporates security requirements and security controls into the system in coordination with functional "end users," information owners, the system administrator, the information system security officer, and the SAISO,

- Ensures that the system is deployed and operated to the agreed-upon security requirements and security controls,

- Assists in the identification, implementation, and assessment of the common security controls, and

- Assists in the completion of the System Reporting Form.

[5] When an agency has not designated a formal Chief Information Officer position, FISMA requires the associated responsibilities to be handled by a comparable agency official.
[6] The role of the information system owner can be interpreted in a variety of ways depending on the particular agency and the system development life cycle phase of the information system. Some agencies may refer to information system owners as program managers or business/asset/mission owners.

Information Owners

The *information owner* is an agency official with statutory or operational authority for specified information and responsibility for establishing the security controls for its generation, collection, processing, dissemination, and disposal. The information owner has the following responsibilities related to system assessments:

- Provides input to information system owners regarding the security requirements and security controls for the information systems where the information resides,
- Assists in the identification and assessment of common security controls where the information resides, and
- Assists in the completion of the System Reporting Form.

Senior Agency Information Security Officer (SAISO)

The SAISO is the agency official responsible for serving as the CIO's primary liaison to the agency's information system owners, and information system security officers. The senior agency information security officer has the following responsibilities related to system and program security assessments:

- Carries out the CIO's responsibilities for system and program security assessments,
- Coordinates the identification, implementation, and assessment of the common security controls,
- Coordinates the assessment of systems with information system owners and information system security officers,
- Conducts assessments of the security program, and
- Possesses professional qualifications, including training and experience required to manage the assessment of systems and the information security program.

Information System Security Officer

The *information system security officer* is the agency official assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program. The information system security officer has the following responsibilities related to system assessments:

- Assists the senior agency information security officer and the system owner in the identification, implementation, and assessment of the common security controls, and

- Assists the senior agency information security officer and the system owner in the assessment of systems.

1.3 History of the Document

In November 2000, NIST prepared the Federal IT Security Assessment Framework issued by the Federal Chief Information Officer (CIO) Council. The Framework provided a method that agencies could employ to routinely evaluate the status of their information system security program and provided the groundwork for standardizing on five levels of security effectiveness and measurements. In November 2001, NIST published NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems" which built upon the Framework by providing seventeen security control areas such as risk management, contingency planning, and data integrity along with numerous questions on specific security controls and techniques that should be implemented on an information system. Additionally, the guide provided a means for reporting the assessment results in the same five levels as in the Framework.

In response to the Government Information Security Reform Act (GISRA) requirement for an annual assessment, in July 2002, the Office of Management and Budget (OMB) required all non-national security systems to undergo a NIST SP 800-26 self-assessment on an annual basis. When FISMA superseded GISRA, the OMB requirement to use NIST SP 800-26 remained.

In September 2002, NIST released the first automated version of the NIST SP 800-26 system questionnaire. The Automated Security Self-Evaluation Tool (ASSET) automated the process of completing a system self-assessment and assisted in aggregating individual system assessments to assist management in developing an agency-wide perspective on the state of their information system security program. ASSET and source code is freely available at http://csrc.nist.gov/asset/.

With the release of NIST SP 800-53, this document is being updated to be consistent with FIPS 199, FIPS 200, and the security controls and concepts contained in NIST SP 800-53.

1.4 Audience

The control objectives and techniques presented in this guide are generic and can be applied to organizations in private and public sectors. This document can be used by all levels of management and by those individuals responsible for information security at the system level and for the information security program at the agency-wide level. Additionally, internal and external auditors may use the completed System Reporting Form to guide their review of the information security program. To perform the examination and testing required to complete the System Reporting Form, the assessor must be familiar with, and able to apply, a core knowledge set of information security basics needed to protect information and systems. In some cases, especially in the area of examining and testing technical security controls employed to protect systems, assessors with specialized technical expertise will be needed to ensure that the answers are reliable in the System Reporting Form.

The completed Information Security Program Assessment Questionnaire will allow the agency CIO, SAISO, and independent assessors to further evaluate the posture of the agency's information security program. The agency-wide program-level questionnaire aggregates the system-level assessment results and provides questions that apply directly to program-level requirements (e.g., appointment of a senior agency information security officer, capital planning and investment control, budget and resource allocation, systems and project inventory), taken from a number of federal requirement sources.

1.5 Structure of the Document

Chapter 1 introduces the document and explains system-level reporting and program-level security assessments. Chapter 2 describes the FIPS 199 categorization and provides a method for determining the system boundaries and criticality of the data. Chapter 3 describes the System Reporting Form. Chapter 4 discusses the security program assessment process. Appendix A contains the System Reporting Form. Appendix B contains the Information Security Program Assessment Questionnaire. Appendix C contains a glossary. Appendix D lists references used in developing this document.

1.6 How This Document Should Be Used

At the system level, this document helps standardize the system security assessment process by serving as the assessment reporting form for the:

- FISMA annual assessment for major information systems,
- Certification documentation,
- Continuous monitoring of selected security controls,
- Preparation for an audit, and
- Identification of resource needs to improve the system's security posture.

FISMA requires that organizations conduct an annual assessment of major information systems (i.e., FIPS 199 moderate- and high-impact systems)[7]. Although FISMA does not require that assessments be conducted on low-impact systems, a completed assessment reporting form serves as the key documentation for the C&A process for low-impact systems.[8] The continuous monitoring of security controls, which is required for all FIPS 199 impact levels, also allows the owners of low-impact systems to more effectively manage the security posture of their information resources during the three-year life span

[7] NIST SP 800-53 requires that assessments are to be performed at least annually on moderate impact and high impact systems, but do not have to be performed annually on low-impact systems.

[8] For specific information on C&A requirements for low-impact systems, see NIST SP 800-37, Guide for the Security *Certification and Accreditation for Federal Information Systems*.

of a system's C&A. Realizing that it is not feasible or cost-effective to monitor all of the security controls in a system on a continuous basis, the system owner should select an appropriate subset of those controls for periodic assessment.

At the agency-wide, security program level, this document should be used to perform an assessment of the information security program. The two-part questionnaire – roll-up of the System Reporting Forms and the program-related questions – will help organizations meet the FISMA requirement to perform an independent evaluation of the information security program and practices to determine their effectiveness.

1.7 Key Factors for Success

A number of key factors must be considered and implemented before a successful system-level reporting process and agency-wide program-level assessment process can begin. Both processes should be properly led, accomplished by the correct personnel, and have clearly identified goals.

1.7.1. Management of the System-Level Reporting Process

The organization should take the following steps to ensure that the system-level reporting process is successful:

- Enter on the assessment reporting form all common security controls before distributing the form,
- Designate a lead management official with responsibility for coordinating the assessment reporting process,
- Establish clear organizational roles and responsibilities,
- Brief key players on the goals and objectives of the assessment reporting process, and
- Establish and maintain good communication among team members during the assessment reporting.

1.7.2 Management of the Program-Level Assessment Process

The organization should take the following steps to ensure that the program-level assessment process is successful:

- Designate a lead management official with responsibility for coordinating the program assessment process,
- Establish clear organizational roles and responsibilities,
- Brief key players as to the goals and objectives of the program assessment process, and

- Establish and maintain good communication among team members during the program assessment.

1.7.3 Using Automation for System Assessment Reporting

Automated tools can be used to support the assessment process, and provide for easier roll-up of data for internal or external reporting. Factors to consider in the use of automated tools include:

- Ascertain the completeness of tool functionality in terms of supporting all components listed in NIST SP 800-26,

- Determine who will have access to the tools, including specific roles and responsibilities,

- Ensure that the system processing the tool is secure and is certified and accredited,

- Provide adequate training for those using the tool(s), and

- Establish technical support capability.

2. System Assessment

The System Reporting Form is a tool for documenting an assessment of the security controls in place for a major application or a general support system. Before a system is assessed, there are key security-related activities that should be completed. An inventory of all systems should be conducted, and then all systems should be categorized according to their impact on the agency's mission. A determination must then be made as to the boundaries of the system, keeping in mind the impact of the information stored within, processed by, or transmitted by the system(s). A completed general support system or major application security plan, which is required under OMB Circular A-130, Appendix III, should describe the boundaries of the system, the impact level of the data, and the security controls in place or planned for the system.

2.1 Systems Inventory and FIPS 199 Categorization

FISMA requires that agencies have in place a system inventory. All systems in the inventory should be categorized using FIPS 199, as a first step in support of the security planning activity and eventually in the assessment of the security controls implemented on the system.

FIPS 199 is the standard to be used by all federal agencies to categorize all information and information systems collected or maintained by, or on behalf of, each agency based on the objectives of providing appropriate levels of information security according to impact. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government, promotes: (i) effective management and oversight of the information security program, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the OMB and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

FIPS 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

The *potential impact* is **LOW** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.[9]

AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii)

[9] Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The *potential impact* is **MODERATE** if—

- The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

  AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The *potential impact* is **HIGH** if—

- The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

  AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

This categorization forms the basis of identification of a minimum set of security controls for the system as documented in NIST SP 800-53. This activity will supplement additional risk assessment activity, which will result in a final determination of the security controls to be applied. As the impact level increases, so do the minimum assurance requirements.

2.2 System Boundaries

Defining the scope of the assessment requires an analysis of system boundaries and organizational responsibilities. Networked systems make the boundaries much harder to define. Many organizations have distributed client-server architectures where servers and workstations communicate through networks. Those same networks are connected to the Internet. A system, as defined in NIST Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Information Systems*, is identified by defining boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a information single system requiring a system security plan, a certification and accreditation, and periodic security assessments or recertification and reaccredidation whenever a major modification to the system occurs.

The process of uniquely assigning information resources[10] to an information system defines the security boundary for that system.

An important element of the assessment will be determining the effectiveness of the boundary controls when the information system is part of a network. The boundary controls must protect the defined system or group of systems from unauthorized intrusions. If such boundary controls are not effective, then the security of the systems under review will depend on the security of the other systems connected to it. In the absence of effective boundary controls, the assessor should determine and document the adequacy of security controls related to each system that is connected to the system under review.

FIPS 199 defines security categories for information systems based on potential impact on organizations or individuals should there be a breach of security—that is, a loss of confidentiality, integrity, or availability. FIPS 199 security categories can play an important part in defining system boundaries by partitioning the agency's information systems according to the criticality or sensitivity of the systems and the importance of those systems in accomplishing the agency's mission. This is particularly important when there are various FIPS 199 impact levels contained in one system. The notion of securing a system to the high watermark or highest impact level must be considered when grouping numerous minor applications/subsystems with varying FIPS 199 impact levels into a single general support system or major application. Having the ability to isolate the high-impact systems will not only result in more secure systems, but will also reduce the amount of resources required to secure many applications/systems that do not require that level of security. See NIST SP 800-18 Revision 1 for additional information on system boundaries.

2.3 Security Controls

NIST SP 800-53 provides a catalog of security controls and guidelines for specifying and selecting controls for information systems supporting the executive agencies of the federal government. The implementation of one of the three minimum security control baselines required for the FIPS 199 impact level, along with applying the assessment criteria contained in NIST SP 800-53A, demonstrate control effectiveness in a consistent and repeatable manner and contributes to the organization’s confidence that there is ongoing compliance with stated security requirements.

2.3.1 Compensating Controls

Compensating security controls are the management, operational, or technical controls employed by an organization, in lieu of prescribed controls in the low, moderate, or high security control baselines, which provide equivalent or comparable protection for an information system. Compensating security controls for an information system will be employed by an organization only under the following conditions: (i) the organization selects the compensating controls from the security control catalog in NIST SP 800-53; (ii) the organization provides a complete and convincing rationale and justification for

[10] Information resources consist of information and related resources, such as personnel, equipment, funds, and information technology.

how the compensating controls provide an equivalent security capability or level of protection for the information system; and (iii) the organization assesses and formally accepts the risk associated with employing the compensating controls in the information system. The use of compensating security controls must be reviewed, documented in the system security plan, and approved by the authorizing official for the information system. The System Reporting Form should also contain a notation; see Section 3.4 for additional information.

2.3.2 Scoping Guidance

Scoping guidance provides organizations with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines. There are several considerations, described below, that can potentially impact how the baseline security controls are applied by the organization. System security plans should clearly identify which security controls employed scoping guidance and include a description of the type of considerations that were made. The System Reporting Form should also contain a notation when scoping guidance is applied. (See Section 3.4 for additional information.) The application of scoping guidelines must be reviewed and approved by the authorizing official for the information system.

Technology-related considerations—

- Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) will only be applicable if those technologies are employed or are required to be employed within the information system.

- Security controls will only be applicable to those components of the information system that typically provide the security capability addressed by the minimum security requirements.[11]

- Security controls that can be either explicitly or implicitly supported by automated mechanisms will not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. In situations where automated mechanisms are not readily available or technically feasible, compensating security controls, implemented through non-automated mechanisms or procedures, will be used to satisfy minimum security requirements.

[11] For example, auditing controls would typically be applied to the components of an information system that provide or are required to provide auditing capability (mainframes, servers, etc.) and would not necessarily be applied to every user-level workstation within the organization. Access control mechanisms would not typically be applied to such devices as personal digital assistants, facsimile machines, printers, pagers, cellular telephones, or other components of an information system that provide limited functionality. Organizations should, however, carefully assess the inventory of components that make up their information systems to determine which security controls are applicable to the various components. As technology advances, increased functionality may be present in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an organizational assessment of risk.

Common security control-related considerations—

- Security controls designated by the organization as common controls will, in most cases, be managed by an organizational entity other than the information system owner. Every control in a security control baseline must be addressed either by the organization through common security controls or by the information system owner. Decisions on common control designations must not, however, affect the organization's responsibility in providing the necessary security controls required to meet the minimum security requirements for the information system. See section 2.3.3 for additional information on common security controls.

Public access information systems-related considerations—

- Security controls associated with public access information systems must be carefully considered and applied with discretion, since some of the security controls from the specified security control baselines (e.g., personnel security controls, identification and authentication controls) may not be applicable to users accessing information systems through public interfaces.[12]

Infrastructure-related considerations—

- Security controls that refer to organizational facilities (e.g., physical access controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) will be applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system (including its information technology assets such as electronic mail or web servers, server farms, data centers, networking nodes, controlled interface equipment, and communications equipment).

Scalability-related considerations—

- Security controls will be scalable by the size and complexity of the particular organization implementing the controls and the impact level of the information system. Scalability addresses the breadth and depth of security control implementation. Discretion is needed in scaling the security controls to the

[12] For example, while the baseline security controls require identification and authentication of organizational personnel who maintain and support information systems that provide public access services, the same controls might not be required for users accessing those systems through public interfaces to obtain publicly available information. On the other hand, identification and authentication must be required for users accessing information systems through public interfaces to access their private/personal information.

particular environment of use to ensure a cost-effective, risk-based approach to security control implementation.[13]

Risk-related considerations—

- Security controls that uniquely support the confidentiality, integrity, or availability security objectives can be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization for the corresponding security objectives of confidentiality, integrity, or availability before moving to the high water-mark;[14] (ii) is supported by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system.[15]

2.3.3 Common Controls

An agency-wide view of the security program facilitates the identification of common security controls that can be applied to one or more agency information systems. Common security controls can apply to: (i) all agency information systems; (ii) a group of information systems at a specific site (sometimes associated with the terms site certification/accreditation); or (iii) common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites (sometimes associated with the terms type certification/accreditation). Common security controls, typically identified during a collaborative agency-wide process with the involvement of the CIO, senior agency information security officer, authorizing officials, information system owners, and information system security officers (and by developmental program managers in the case of common security controls for common hardware, software, and/or firmware), have the following properties:

- The development, implementation, and assessment of common security controls can be assigned to responsible agency officials or organizational elements (other

[13] For example, a contingency plan for a large and complex organization with a moderate-impact or high-impact information system may be quite lengthy and contain a significant amount of implementation detail. In contrast, a contingency plan for a smaller organization with a low-impact information system may be considerably shorter and contain much less implementation detail.

[14] When employing the "high water-mark" concept, some of the security objectives (i.e., confidentiality, integrity, or availability) may have been increased to a higher impact level. As such, the security controls that uniquely support these security objectives will have been upgraded as well. Consequently, organizations must consider appropriate and allowable downgrading actions to ensure cost-effective, risk-based application of security controls.

[15] Information that is security-relevant at the system level (e.g., password files, network routing tables, cryptographic key management information) must be distinguished from user-level information within an information system. Certain security controls within an information system are used to support the security objectives of confidentiality and integrity for both user-level and system-level information. Organizations must exercise caution in downgrading confidentiality or integrity-related security controls to ensure that the downgrading action does not affect the security-relevant information within the information system.

than the information system owners whose systems will implement or use those common security controls); and

- The results from the assessment of the common security controls can be used to support the security certification and accreditation processes of agency information systems where those controls have been applied.

Many of the management and operational security controls (e.g., contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, and physical security controls) needed to protect an information system may be excellent candidates for common security control status. The objective is to reduce security costs by centrally managing the development, implementation, and assessment of the common security controls designated by the agency—and subsequently, sharing assessment results with the owners of information systems where those common security controls are applied. Security controls not designated as common controls are considered *system-specific controls* and are the responsibility of the information system owner. System security plans should clearly identify which security controls have been designated as common security controls and which controls have been designated as system-specific controls. The System Reporting Form should also identify which controls are common controls; see Section 3.4 for additional information.

Organizations may also assign a hybrid status to security controls in situations where one part of the control is deemed to be common, while another part of the control is deemed to be system-specific. For example, an organization may view the IR-1 (Incident Response Policy and Procedures) security control as a hybrid control with the policy portion of the control deemed to be common and the procedures portion of the control deemed to be system-specific. Hybrid security controls may also serve as templates for further control refinement. An organization may choose, for example, to implement the CP-2 (Contingency Plan) security control as a master template for a generalized contingency plan for all organizational information systems with individual information system owners tailoring the plan, where appropriate, for system-specific issues.

Information system owners are responsible for any system-specific issues associated with the implementation of an organization's common security controls. These issues are identified and described in the system security plans for the individual information systems and should be assessed and the results of the assessment detailed or referenced in the reporting form. The SAISO, acting on behalf of the CIO, should coordinate with organizational officials (e.g., facilities managers, site managers, personnel managers) responsible for the development and implementation of the designated common security controls to ensure that the required controls are put into place, the controls are assessed, and the assessment results are shared with the appropriate information system owners.

Partitioning security controls into common security controls and system-specific security controls can result in significant savings to the organization in control development and implementation costs. It can also result in a more consistent application of the security controls across the organization at large. Moreover, equally significant savings can be realized in the security certification and accreditation process. Rather than assessing common security controls in every information system, the certification process draws upon any applicable results from the most current assessment of the common security controls performed at the organization level. An agency-wide approach to reuse and share assessment results can greatly enhance the efficiency of the annual FISMA assessments and the security certifications and accreditations being conducted by organizations, and significantly reduce security program costs.

While the concept of security control partitioning into common security controls and system-specific controls is straightforward and intuitive, the application of this principle within an organization takes planning, coordination, and perseverance. If an organization is just beginning to implement this approach or has only partially implemented this approach, it may take some time to get the maximum benefits from security control partitioning and the associated reuse of assessment evidence. Because of the potential dependence on common security controls by many of an organization's information systems, a failure of such common controls may result in a significant increase in agency-level risk—risk that arises from the operation of the systems that depend on these controls.

3. System Reporting Form Structure

The System Reporting Form (see Appendix A) contains three sections: cover sheet, reporting form, and notes. The cover sheet requires descriptive information about the major application, general support system, or group of interconnected systems being assessed. The cover sheet also requires that the FIPS 199 impact level (i.e., high, moderate, low) be documented for each of the three security objectives (i.e., confidentiality, integrity, availability). The System Reporting Form contains each of the seventeen control families contained in NIST SP 800-53 and SP 800-53A.

The System Reporting Form may be customized by the organization. An organization can add more security controls to those listed for each control family, require more descriptive information, and even pre-mark certain security controls if applicable. For example, many agencies may have common controls (e.g., personnel security procedures, physical security procedures, awareness and training) that apply to all systems within the agency. The Level 1 (Policy) and Level 2 (Procedures) columns in the reporting form can be pre-marked to reflect the existence of agency-wide policy and procedures. There may also be specific common controls that are implemented and tested in a centralized manner. If so, the Level 3 (Implemented) and Level 4(Tested) columns can be pre-marked as well. Additional columns may be added to reflect the status of the control, e.g., planned action date, or location of documentation. The System Reporting Form should not have security controls removed or modified to reduce the effectiveness of the control.[16]

At the end of each control family, there is an area provided for notes. This area may be used for denoting where in a system security plan specific sections should be modified. It can be used to document the justification as to why a security control is not being implemented fully (e.g., existence of compensating controls) or why it is overly rigorous. The note section may be a good place to mark where follow-up is needed or additional testing, such as penetration testing or product evaluations, needs to be initiated. Additionally, the note section may reference supporting documentation on how the security controls were tested and a summary of findings.

3.1 System Reporting Form Cover Sheet

This section provides instruction on completing the System Reporting Form cover sheet, standardizing on how the completed evaluation should be marked, how systems are titled, and assigning/documenting the FIPS 199 impact level of the system.

3.1.1 System Identification

The cover page of the System Reporting Form begins with the name and title of the system to be assessed. As explained in NIST SP 800-18 Revision 1, each major application or general support system should be assigned a unique name/identifier. Assigning a unique identifier to each system helps to ensure that appropriate security

[16] If a security control is not employed because a compensating control (or controls) has been implemented, this should be documented in the notes at the end of the security control family section.

requirements are met based on the unique requirements for the system, and that allocated resources are appropriately applied.

In many cases, the major application or general support system will contain interconnected systems. The connected systems should be listed, along with the date when the system was certified and accredited. A determination should be made and noted on the cover sheet as to whether the boundary controls are effective. If the boundary controls are not effective, planned action(s) should be identified on the cover sheet.

The line below the system name and title requires the assessor to mark the system category (general support or major application). If an agency has additional system types or system categories, i.e., mission-critical or non-mission-critical, the cover sheet should be customized to include them.

3.1.2 Purpose and Assessor Information

The purpose and objectives of the assessment should be identified. For example, the assessment may have been performed to satisfy the annual FISMA reporting requirement, to document a C&A, to assess the security posture of a system after changes have been made, or to document the continuous monitoring of a system.

The name, title, and organizational affiliation of the individuals who perform the assessment should be listed. The organization should customize the cover page accordingly.

The start date and completion date of the evaluation should be listed. The length of time required to complete an assessment will vary depending on the purpose of the assessment.

3.1.3 FIPS 199 Impact Level

The impact level of the system, as determined by the authorizing official, SAISO, and system owner, should be documented on the FIPS 199 Impact Level table on the reporting form cover sheet and also at the beginning of each security control family.

3.2 Security Control Families and Security Controls

There are seventeen families of controls in the System Reporting Form. Each control family, and each set of controls within each family, is identified in this publication exactly as they are documented in NIST SP 800-53 and NIST SP 800-53A. Each control family also has the same identifier used in NIST SP 800-53 and NIST SP 800-53A. For example, the identifier for the Access Control family is AC; the identifier for the Configuration Management family is CM. Each control family is also assigned to a security control class (i.e., management, operational, technical). (See Figure 2 for each security control family name, security control identifier, and security control family class.)

Control Family Name	**Identifier**	**Class**
Access Control	AC	Technical
Audit and Accountability	AU	Technical
Awareness and Training	AT	Operational
Certification, Accreditation, and Security Assessments	CA	Management
Configuration Management	CM	Operational
Contingency Planning	CP	Operational
Identification and Authentication	IA	Technical
Incident Response	IR	Operational
Maintenance	MA	Operational
Media Protection	MP	Operational
Personnel Security	PS	Operational
Physical and Environmental Protection	PE	Operational
Planning	PL	Management
Risk Assessment	RA	Management
System and Communications Protection	SC	Technical
System and Information Integrity	SI	Operational
System and Services Acquisition	SA	Management

Figure 2. Security Control Families, Identifiers, and Classes

Each control family is comprised of a number of controls. Some control families have as few as four controls; some control families have as many as twenty controls. In the System Reporting Form, each control family has its own section and within each control family section, each control has a row in which the results of the assessment are to be documented.

At the top of each control family section the security control class is identified and the information system’s FIPS 199 impact level should be entered. The impact level should have been documented in the system security plan, and used to select the baseline set of security controls.

Each security control has a row of cells in which the assessor must document the results of the assessment. To aid the assessor, under each security control name is a box that contains the control identifier and any control enhancements that were to be implemented for low-, moderate-, or high-impact systems. For example, among the twenty controls in the Access Control family is control AC-2 – Account Management. In Figure 3, AC-2 Account Management contains a box with three segments:

- The left-most segment is labeled “LOW” and contains “AC-2.” This indicates that for a system with a FIPS 199 low-impact level, the security control is to be implemented as documented in NIST SP 800-53 (and assessed using the guidance in NIST SP 800-53A).

- The center segment is labeled "MOD" and contains "AC-2 (1) (2) (3)." This indicates that for a system with a FIPS 199 moderate-impact level, the security control is to be implemented as documented in NIST SP 800-53 using the first three of four control enhancements that are documented in NIST SP 800-53. (These control enhancements are documented in NIST 800-53 using parentheses; this convention is continued in this publication.)

- The right-most segment is labeled "HIGH" and contains "AC-3 (1) (2) (3) (4)." This indicates that for a system with a FIPS 199 high-impact level, the security control is to be implemented as documented in NIST SP 800-53 using all four of the control enhancements that are documented in NIST SP 800-53.

Security Control	L.1	L.2	L.3	L.4	L.5	Common Control	Compensating Control	Scoping Guidance Applied
AC-1 Access Control Policy and Procedures **LOW** AC-1 **MOD** AC-1 **HIGH** AC-1								
AC-2 Account Management **LOW** AC-2 **MOD** AC-2 (1) (2) (3) **HIGH** AC-2 (1) (2) (3) (4)								

Figure 3. Sample System Reporting Form

3.3 Five Levels of Security Effectiveness

In order to better understand the five levels of security effectiveness as key parts of the assessment reporting process, it is important to understand their origin – the Federal IT Security Assessment Framework. The Framework was developed by the Federal CIO Council and was published in November 2000. It was included as an appendix to the original NIST SP 800-26, published in November 2001. The complete Framework can be found at *http://csrc.nist.gov/policies/index.html*.

3.3.1 Five Levels in Detail

The Framework is divided into five levels: Level 1 of the Framework reflects that a system has documented security policy. At Level 2, the system also has documented procedures and controls to implement the policy. Level 3 indicates that procedures and controls have been implemented. Level 4 shows that the procedures and controls are tested and reviewed. At Level 5, the system has procedures and controls fully integrated into a comprehensive program. Each level represents a more complete and effective security program. Figure 4 shows the five levels.

Level 1	Documented Policy
Level 2	Documented Procedures
Level 3	Implemented Procedures and Controls
Level 4	Tested and Reviewed Procedures and Controls
Level 5	Fully Integrated Procedures and Controls

Figure 4. Levels of Security Effectiveness

Level 1 – Policy – includes:

- Formally documented and disseminated security policy covering agency headquarters and major components (e.g., bureaus and operating divisions). The policy may be system-specific.
- Policy that references most of the basic requirements and guidance issued from applicable public laws; other federal, department, and agency policy; and applicable NIST guidelines.

A system is at Level 1 if there is a formal, up-to-date, and documented policy that establishes a continuing cycle of assessing risk, implements effective security policies including training, and uses monitoring for program effectiveness. Such a policy may include major agency components, (e.g., bureaus and operating divisions) or specific assets.

A documented security policy is necessary to ensure adequate and cost-effective organizational and system security controls. A sound policy delineates the security management structure and clearly assigns security responsibilities, and lays the foundation necessary to reliably measure progress and compliance.

Level 2 – Procedures – includes:

- Formal, complete, well-documented procedures for implementing policies established at Level 1.
- The basic requirements and guidance issued from applicable public laws; other federal, department, and agency policy; and applicable NIST guidelines.

A system is at Level 2 when formally documented procedures are developed that focus on implementing specific security controls. Formal procedures promote the continuity of the security program. Formal procedures also provide the foundation for a clear, accurate, and complete understanding of the program implementation. An understanding of the risks and related results should guide the strength of the control and the corresponding procedures. The procedures document the implementation of and the rigor in which the control is applied. Level 2 requires procedures for a continuing cycle of assessing risk and vulnerabilities, implementing effective security policies, and monitoring effectiveness of the security controls. Approved system security plans are in place for all systems. Well-documented and current security procedures are necessary to ensure that adequate and cost-effective security controls are implemented.

Level 3 – Implemented – includes:

- Security procedures and controls that are implemented.
- Procedures that are communicated and individuals who are required to follow them.

At Level 3, the information security procedures and controls are implemented in a consistent manner and reinforced through awareness and training. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. Security controls for a system could be implemented and not have procedures documented, but the addition of formal documented procedures at Level 2 represents a significant step in the effectiveness of implementing procedures and controls at Level 3. While testing the ongoing effectiveness is not emphasized in Level 3, some testing is needed when initially implementing controls to ensure they are operating as intended.

Level 4 – Tested – includes:

- Routinely evaluating the adequacy and effectiveness of security policies, procedures, and controls.
- Ensuring that effective corrective actions are taken to address identified weaknesses, including those identified as a result of potential or actual security incidents or through security alerts issued by federal organizations, vendors, and other trusted sources.

Routine assessments and response to identified vulnerabilities are important elements of risk management, which includes identifying, acknowledging, and responding, as appropriate, to changes in risk factors (e.g., computing environment, impact levels) and ensuring that security policies and procedures are appropriate and are operating as intended on an ongoing basis.

Routine assessments are an important means of identifying inappropriate or ineffective security procedures and controls, reminding employees of their security-related responsibilities, and demonstrating management's commitment to security. Assessments can be performed by agency staff, contractors, or others engaged by agency management. Independent audits, such as those arranged by the General Accountability Office (GAO) or an agency Inspector General (IG), are an important check on agency performance, but should not be viewed as a substitute for assessments initiated by agency management.

To be effective, routine assessments must include tests and examinations of security controls. Reviews of documentation, walk-through of agency facilities, and interviews with agency personnel, while providing useful information, are not sufficient to ensure that controls, especially computer-based controls, are operating effectively. Examples of tests that should be conducted are network scans to identify known vulnerabilities, analyses of router and switch settings and firewall rules, reviews of other system software settings, and tests to see if unauthorized system access is possible (penetration testing). Tests performed should consider the risks of authorized users exceeding authorization as well as unauthorized users (e.g., external parties, hackers) gaining access. Similar to Levels 1 through 3, to be meaningful, assessments must include security controls of interconnected assets, e.g., network supporting applications being tested.

When systems are first implemented or are modified, they should be tested and certified to ensure that the security controls are initially operating as intended. (This would occur at Level 3.) Requirements for subsequent testing and recertification should be integrated into an agency's ongoing test and assessment program.

In addition to test results, agency assessments should consider information gleaned from records of potential and actual security incidents and from security alerts, such as those issued by software vendors. Such information can identify specific vulnerabilities and provide insights into the latest threats and resulting risks.

Level 5 – Integrated – includes:

- A comprehensive security program that is an integral part of an agency's organizational culture.

- Decision-making based on cost, risk, and mission impact.

The consideration of information security is pervasive in the culture of a Level 5 system. A proven life-cycle methodology is implemented and enforced, and an ongoing program to identify and institutionalize best practices has been implemented. There is active support from senior management. Decisions and actions that are part of the system life cycle include:

- Improving security program,
- Improving security program procedures,
- Improving or refining security controls,
- Integrating security within existing and evolving IT architecture, and
- Improving mission processes and risk management activities.

Each of these decisions results from a continuous improvement and refinement program instilled within the organization. At Level 5, the understanding of mission-related risks and the associated costs of reducing these risks are considered with a full range of implementation options to achieve maximum mission cost-effectiveness of security measures.

3.3.2 Five Levels and Assessment Reporting

In order to properly document the effectiveness of each selected and implemented control in the assessment process, the five levels of security effectiveness are provided in the System Reporting Form.

The method for completing the assessment can be based entirely on the guidance contained in NIST SP 800-53A. Supporting documentation describing what has been tested and the results of the tests add value to the assessment and will make the next review of the system easier.

Once the reporting form is completed for the first time, future assessments of the system will require considerably less effort. The completed assessment form should establish a baseline. If this year's assessment indicates that most of the security controls in place are at Level 2 or Level 3, then that would be the starting point for the next assessment. More time can be spent identifying ways to increase the level of effectiveness instead of having to gather all the initial information again. Use the notes section at the end of each control family to list whether there is supporting documentation and for any lengthy explanations.

The assessor must annotate on the System Reporting Form the results of the assessment, checking whether there are documented policies (Level 1), procedures for implementing the control (Level 2), the control has been implemented (Level 3), the control has been tested and if found ineffective, remedied (Level 4), and whether the control is part of an agency's organizational culture (Level 5).

The policy and procedures for a security control can be found at the department level, agency level, agency component level, system level, or application level. If a topic area is documented at a high level in policy, the Level 1 (Policy) box should be checked in the reporting form. If there are additional lower-level policies for the system, describe what was reviewed in the notes section at the end of the control family. If a control is described in detail in procedures, and implemented, the Level 2 (Procedures) and Level 3 (Implemented) boxes should be checked in the System Reporting Form. Testing and reviewing controls are an essential part of securing a system. For each control, check whether it has been tested and/or reviewed when a significant change occurred.

Since the five levels represent a measure of the maturity of the security function of a system, there is a hierarchical and dependent relationship between each of the levels.

- Level 1 (Policy) must be in place before Level 2 (Procedures) can be assessed as being in place.

- Level 2 (Procedures) must be developed before Level 3 (Implemented) can be achieved.

- Level 3 (Implemented) must be accomplished before Level 4 (Tested) can be assessed as being in place.

- Level 4 (Tested) must be complete before Level 5 (Integrated) can be accomplished.

Some fields in the System Reporting Form have been shaded because they do not have to be completed. These fields are in the Level 1 (Policy) column of Appendix A. All fields in this column except for the first control in each control family are shaded because the first control (e.g., AC-1, AU-1 . . . SI-1) in each control family only relates to policy. The remaining controls do not apply at the policy level. The shaded fields in the reporting form do not require a check mark.

There may be instances in which an organization may want to shade (and not complete) specific fields in the Level 5 (Integrated) column of the reporting form. In these instances, the scope of a security control may be so finite or focused, as implemented for that system, that even when implemented and successfully tested, there may be no way to measure its impact on the organization's culture. For example, control AC-11 (Access Control, Session Lock) or IA-6 (Identification and Authentication, Authenticator Feedback) may be so focused that the implementation and successful testing of that control may have no bearing on a Level 5 posture of the system or organization. The organization's security staff may make such a determination before passing the reporting form to the system owner and/or system security officer. Conversely, the system owner and/or system security officer may meet with the security staff during or after the completion of the reporting form to discuss the applicability of Level 5 to that control.

The five levels describing the effectiveness of the security control provide a picture of the security posture, maturity, or effectiveness, of each control; however, how well each one of these security controls is met is still subjective.

3.4 Common Controls, Compensating Controls, and Scoping Guidance Fields

In addition to the fields for each of the five levels of security effectiveness in the System Reporting Form, there are three other fields to be considered:

Common Control. This gives the organization security staff the opportunity to pre-answer the reporting form before sending it to system owners, system security officers, or other assessors for completion. The "common control" field is to be used in those cases in which the control is not managed or implemented by the system owner and/or system security officer, but is centrally managed, either agency-wide or by another organizational entity. If additional space is needed, clearly link the comment in the "common control" field to the notes section at the end of the control family.

Compensating Control. The "compensating control" field is to be marked for the control when: 1) a control has not been implemented because another control which provides equal or comparable protection has been implemented, and 2) the compensating control has been implemented.

Both the compensating control and the control being compensated should be documented in the respective "compensating control" fields. If additional space is needed, clearly link the comments in the "compensating control" fields to the notes section at the end of the control family.

Scoping Guidance Applied. This field is to be used to document instances in which organizations further tailor or fine-tune the implementation of security controls, based on the specific scoping guidance considerations contained in Section 3.3 of NIST SP 800-53. The “scoping guidance applied” field should contain detailed information that describes which of the scoping guidance considerations were employed, the impact on the control, and if other security controls were implemented or enhanced to compensate for this decision. If additional space is needed, clearly link the comments to the notes section at the end of the control family.

Effectiveness Level Reached. At the end of each control family section, the effectiveness levels (Level 1 through Level 5) can be checked if all applicable security controls have obtained that level. A level can only be obtained if the preceding level is reached. For example, an information system cannot implement the security controls (Level 3) if there are no procedures (Level 2) documenting how the control should be implemented. The total at the end of each section will assist in the roll-up at the agency-wide program level.

3.5 Conclusion

The System Reporting Form can be used for two purposes. First, it can be used by agency managers who know their systems and security controls to quickly gain a general understanding of where security improvements for a system, group of systems, or the entire agency need to be made. Second, it can be used as a guide for thoroughly evaluating the status of security for a system. The results of such thorough reviews provide a much more reliable measure of security effectiveness and may be used to: 1) fulfill FISMA and the organization’s internal reporting requirements; 2) support the C&A process for the system; 3) support the continuing monitoring requirement; 4) prepare for audits; and 5) identify resource needs to improve the system’s security posture.

3.5.1 System Reporting Form Analysis

The owners of the system and the authorizing official are responsible for securing the system. The SAISO should work closely with the system owner and the authorizing official to review assessment results and findings. A plan of action and milestones (POA&M) and the system security plan should be updated to reflect the results of the analysis.

3.5.2 Plan of Action and Milestones

A POA&M should include documentation on how the implementation of, or enhancement to, a security control is to be implemented (e.g., specific procedures written, equipment installed and tested, personnel trained). The action plan must contain projected dates, evidence of an allocation of resources, and follow-up reviews to ensure that remedial actions have been effective. Quarterly updates should be submitted to the CIO to assist in the preparation of the quarterly POA&M submission to OMB.

4. Program Assessments

FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials and CIOs to conduct annual reviews of the agency's information security program and report the results to OMB. OMB uses this data to assist in its oversight responsibilities and to prepare an annual report to Congress on agency compliance with the Act.

In addition, FISMA requires each agency to have conducted an independent evaluation of its information security program each year. For agencies having an IG, that evaluation is to be done by the agency IG. For agencies not having an IG, the evaluation is to be done by an external auditor. In either case, the agency annual report to OMB must include the independent evaluation.

Each quarter, agencies prepare and submit POA&M reports to OMB for all programs and systems where an information system security weakness has been found. Additionally, program officials shall regularly (at the direction of the CIO) update the agency CIO on their program to enable the CIO to monitor agency-wide remediation efforts and provide the quarterly update of the POA&M to OMB.

This program assessment questionnaire will assist an agency in the completion of the annual report and in the preparation of the quarterly POA&Ms.

4.1 Program Questionnaire Structure

The program assessment questionnaire contains three sections: Cover sheet, Part 1 *Agency System Assessment Report Results,* and Part 2 *Agency Information Security Program Questions.*

4.1.1 Program Questionnaire Cover Sheet

The cover sheet requires descriptive information such as the name of the agency, bureau or agency-operating unit, and the name, title and organization of the individual completing the questionnaire. The date and time period covered in the report should be listed along with describing the purpose of the assessment. For example, the annual assessment of the agency information security program is required by FISMA; an assessment was performed because of repeated virus infections. The final information listed on the cover sheet is the number of agency systems in the low, moderate, and high FIPS 199 impact categories.

4.1.2 Part 1 - System Assessment Report Results Consolidation

Part 1 aggregates the system-level assessments into a single row for each of the seventeen control families in NIST SP 800-53. The system control family status for any effectiveness Level 1 (Policy) through Level 5 (Integrated) is reached if all the security controls in a family have been implemented or negated through scoping guidance for every system in the agency. For example, Level 3 (Implemented) is reached if all security controls in the control family have been implemented on a system.

The Level 1 (Policy) and Level 2 (Procedures) columns typically are answered at the agency information security program level since policy and procedures are normally developed at the agency level. For Level 3 (Implemented), Level 4 (Testing), and Level 5 (Integrated), summary data of all the System Reporting Forms are entered based on the FIPS 199 impact levels of agency systems. For example, if there are 100 systems with a FIPS 199 impact level of "Low," and 70 of those systems have implemented all the security controls in the Access Control (AC) family listed in the SP 800-53 Low Baseline, the entry for the Access Control in column Level 3 – Low, would be 70% (indicating 70% have implemented this control family). The same process would be used to aggregate the data for systems in the moderate- and high-impact categories for the Access Control family. This pattern would be followed to complete the table for each of the remaining 16 control families. Below is a diagram depicting the completed Access Control family.

Does the agency at the policy and procedures level and does every system at the implemented, tested, and integrated level meet the minimum security controls in the following control families?	**L.1**	**L.2**	**L.3**			**L.4**			**L.5**			**Comments**
Insert # of systems at Low (L), Moderate (M), High (H) FIPS 199 Impact Levels			**L** **100**	**M** **15**	**H** **2**	**L** **100**	**M** **15**	**H** **2**	**L** **100**	**M** **15**	**H** **2**	
1. (AC) Access Control	100%	100%	70%	100%	100%	70%	100%	100%	10%	10%	10%	

4.1.3 Part 2 – Information Security Program Questions

Part 2 consists of questions related to the management of an agency-wide information security program. Each of these questions addresses information security program elements critical to the success of an agency information security program. This section is flexible and extensible. The agency may add as many questions as desired to more fully assess the status and/or effectiveness of the agency information security program or to address questions or concerns that are raised by other interested parties.

Each question should be answered "Yes" or "No." To answer "Yes," the topic should be documented in agency policy and in detailed procedures, verified by examining the procedures and program area documentation, and interviewing key personnel to determine that the procedures are implemented. If the answer to a question is "No," an explanation should be provided in the comments area and an entry into the agency POA&M should be made describing the resources required and the expected timeframe to mitigate the issue.

4.2 Utilizing the Completed Program Questionnaire

Reporting requests vary in the amount of detail that is required and in the type of information that should be reported. The completed System Reporting Forms are a useful resource for compiling agency reports. The results of the completed seventeen control families can be used to summarize an agency's implementation of security controls.

For the report to present a more complete picture, the results may be summarized by FIPS 199 impact level, not merely totaled into an overall agency grade level. For example, ten systems were assessed. Five of the ten systems assessed were categorized as a FIPS 199 low-impact level; the other five were categorized at the moderate-impact level. The summary would separate the systems into low- and moderate-impact levels. By separating them into groups according to impact level, the report stresses which systems and which control families require more attention based on sensitivity and criticality. Not all systems require the same level of protection; the report should reflect that diversity.

The responses to the questions in Part 2 allow the agency to assess compliance with management-related requirements in FISMA and other guidance such as the Information Technology Management Reform Act of 1996, which requires agencies to implement a formal capital planning and investment control process. The responses can be used to complete the annual OMB FISMA report as well as provide input to any other management-related reports required internally or externally.

Appendix A

System Questionnaire

Table of Contents

System Name, Title, and Unique Identifier: ____

Major Application ____________________ **or** **General Support System** __________________

Name of Assessors: ____

____

____

Date of Assessment: _________________________

List of Connected Systems:

Name of System	**Are boundary controls effective?**	**Certification/Accreditation Date**	**Planned action if not effective**
1.			
2.			
3.			

Security Objectives	**FIPS 199 Impact Level High, Moderate, or Low**
Confidentiality	
Integrity	
Availability	

FIPS 199 Impact Level (based on highest value of security objective impact level): ______________

Purpose and Objective of Assessment: ____

____

____

1. Access Control *Class: Technical*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must limit: (i) information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems); and (ii) the types of transactions and functions that authorized users are permitted to exercise.

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
AC-1 Access Control Policy and Procedures **LOW** AC-1 **MOD** AC-1 **HIGH** AC-1								
AC-2 Account Management **LOW** AC-2 **MOD** AC-2 (1) (2) (3) **HIGH** AC-2 (1) (2) (3) (4)								
AC-3 Access Enforcement **LOW** AC-3 **MOD** AC-3 (1) **HIGH** AC-3 (1)								
AC-4 Information Flow Enforcement **LOW** Not Selected **MOD** AC-4 **HIGH** AC-4								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
AC-5 Separation of Duties **LOW** Not Selected **MOD** AC-5 **HIGH** AC-5								
AC-6 Least Privilege **LOW** Not Selected **MOD** AC-6 **HIGH** AC-6								
AC-7 Unsuccessful Login Attempts **LOW** AC-7 **MOD** AC-7 **HIGH** AC-7								
AC-8 System Use Notification **LOW** AC-8 **MOD** AC-8 **HIGH** AC-8								
AC-9 Previous Logon Notification **LOW** Not Selected **MOD** Not Selected **HIGH** Not Selected								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
AC-10 Concurrent Session Control **LOW** Not Selected **MOD** Not Selected **HIGH** AC-10								
AC-11 Session Lock **LOW** Not Selected **MOD** AC-11 **HIGH** AC-11								
AC-12 Session Termination **LOW** Not Selected **MOD** AC-12 **HIGH** AC-12								
AC-13 Supervision and Review – Access Control **LOW** AC-13 **MOD** AC-13 **HIGH** AC-13 (1)								
AC-14 Permitted Actions Without Identification or Authentication **LOW** AC-14 **MOD** AC-14 (1) **HIGH** AC-14 (1)								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
AC-15 Automated Marking **LOW** Not Selected **MOD** Not Selected **HIGH** AC-15								
AC-16 Automated Labeling **LOW** Not Selected **MOD** Not Selected **HIGH** Not Selected								
AC-17 Remote Access **LOW** AC-17 **MOD** AC-17 (1) (2) (3) **HIGH** AC-17 (1) (2) (3)								
AC-18 Wireless Access Restrictions **LOW** Not Selected **MOD** AC-18 (1) **HIGH** AC-18 (1)								
AC-19 Access Control for Portable and Mobile Systems **LOW** Not Selected **MOD** AC-19 **HIGH** AC-19 (1)								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
AC-20 Personally Owned Information Systems **LOW** AC-20 **MOD** AC-20 **HIGH** AC-20								
Effectiveness Level Reached								

NOTES:

2. Awareness and Training *Class: Operational*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

	L.1	**L.2**	**L.3**	**L.4**	**L.5**	**Common**	**Compensating**	**Scoping Guidance**
Security Control	**Policy**	**Procedures**	**Implemented**	**Tested**	**Integrated**	**Control**	**Control**	**Applied**
AT-1 Security Awareness and Training Policy and Procedures **LOW** AT-1 **MOD** AT-1 **HIGH** AT-1								
AT-2 Security Awareness **LOW** AT-2 **MOD** AT-2 **HIGH** AT-2								
AT-3 Security Training **LOW** AT-3 **MOD** AT-3 **HIGH** AT-3								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
AT-4 Security Training Records **LOW** AT-4 | **MOD** AT-4 | **HIGH** AT-4								
Effectiveness Level Reached								

NOTES:

3. Audit and Accountability *Class: Technical*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
AU-1 Audit and Accountability Policy and Procedures **LOW** AU-1 **MOD** AU-1 **HIGH** AU-1								
AU-2 Auditable Events **LOW** AU-2 **MOD** AU-2 **HIGH** AU-2								
AU-3 Content of Audit Records **LOW** AU-3 **MOD** AU-3 (1) **HIGH** AU-3 (1) (2)								
AU-4 Audit Storage Capacity **LOW** AU-4 **MOD** AU-4 **HIGH** AU-4								

<table>
<tr><th>Security Control</th><th>L.1
Policy</th><th>L.2
Procedures</th><th>L.3
Implemented</th><th>L.4
Tested</th><th>L.5
Integrated</th><th>Common
Control</th><th>Compensating
Control</th><th>Scoping Guidance
Applied</th></tr>
<tr><td><b>AU-5 Audit Processing</b><table><tr><td><b>LOW</b>
AU-5</td><td><b>MOD</b>
AU-5</td><td><b>HIGH</b>
AU-5 (1)</td></tr></table></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>AU-6 Audit Monitoring, Analysis, and Reporting</b><table><tr><td><b>LOW</b>
Not Selected</td><td><b>MOD</b>
AU-6</td><td><b>HIGH</b>
AU-6 (1)</td></tr></table></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>AU-7 Audit Reduction and Report Generation</b><table><tr><td><b>LOW</b>
Not Selected</td><td><b>MOD</b>
AU-7</td><td><b>HIGH</b>
AU-7 (1)</td></tr></table></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>AU-8 Time Stamps</b><table><tr><td><b>LOW</b>
Not Selected</td><td><b>MOD</b>
AU-8</td><td><b>HIGH</b>
AU-8</td></tr></table></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>AU-9 Protection of Audit Information</b><table><tr><td><b>LOW</b>
AU-9</td><td><b>MOD</b>
AU-9</td><td><b>HIGH</b>
AU-9</td></tr></table></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
AU-10 Non-repudiation **LOW** Not Selected **MOD** Not Selected **HIGH** Not Selected								
AU-11 Audit Retention **LOW** AU-11 **MOD** AU-11 **HIGH** AU-11								
Effectiveness Level Reached								

NOTES:

4. Certification, Accreditation, and Security Assessments *Class: Management*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the security controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the security controls.

Security Control	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Common Control**	**Compensating Control**	**Scoping Guidance Applied**
CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures **LOW** CA-1 **MOD** CA-1 **HIGH** CA-1								
CA-2 Security Assessments **LOW** Not Selected **MOD** CA-2 **HIGH** CA-2								
CA-3 Information System Connections **LOW** CA-3 **MOD** CA-3 **HIGH** CA-3								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
CA-4 Security Certification **LOW** CA-4 **MOD** CA-4 **HIGH** CA-4								
CA-5 Plan of Action and Milestones **LOW** CA-5 **MOD** CA-5 **HIGH** CA-5								
CA-6 Security Accreditation **LOW** CA-6 **MOD** CA-6 **HIGH** CA-6								
CA-7 Continuous Monitoring **LOW** CA-7 **MOD** CA-7 **HIGH** CA-7								
Effectiveness Level Reached								

NOTES:

5. Configuration Management *Class: Operational*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems; (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems; and (iii) monitor and control changes to the baseline configurations and to the constituent components of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Security Control	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Common Control**	**Compensating Control**	**Scoping Guidance Applied**
CM-1 Configuration Management Policy and Procedures **LOW** CM-1 **MOD** CM-1 **HIGH** CM-1								
CM-2 Baseline Configuration **LOW** CM-2 **MOD** CM-2 (1) **HIGH** CM-2 (1) (2)								
CM-3 Configuration Change Control **LOW** Not Selected **MOD** CM-3 **HIGH** CM-3 (1)								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
CM-4 Monitoring Configuration Changes **LOW** Not Selected **MOD** CM-4 **HIGH** CM-4								
CM-5 Access Restrictions for Change **LOW** Not Selected **MOD** CM-5 **HIGH** CM-5 (1)								
CM-6 Configuration Settings **LOW** CM-6 **MOD** CM-6 **HIGH** CM-6 (1)								
CM-7 Least Functionality **LOW** Not Selected **MOD** CM-7 **HIGH** CM-7 (1)								
Effectiveness Level Reached								

NOTES:

6. Contingency Planning *Class: Operational*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
CP-1 Contingency Planning Policy and Procedures **LOW** CP-1 **MOD** CP-1 **HIGH** CP-1								
CP-2 Contingency Plan **LOW** CP-2 **MOD** CP-2 (1) **HIGH** CP-2 (1)								
CP-3 Contingency Training **LOW** Not Selected **MOD** CP-3 **HIGH** CP-3 (1)								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
CP-4 Contingency Plan Testing **LOW** Not Selected **MOD** CP-4 (1) **HIGH** CP-4 (1) (2)								
CP-5 Contingency Plan Update **LOW** CP-5 **MOD** CP-5 **HIGH** CP-5								
CP-6 Alternate Storage Sites **LOW** Not Selected **MOD** CP-6 (1) **HIGH** CP-6 (1) (2) (3)								
CP-7 Alternate Processing Sites **LOW** Not Selected **MOD** CP-7 (1) (2) (3) **HIGH** CP-7 (1) (2) (3) (4)								
CP-8 Telecommunications Services **LOW** Not Selected **MOD** CP-8 (1) (2) **HIGH** CP-8 (1) (2) (3) (4)								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
CP-9 Information System Backup **LOW** CP-9 **MOD** CP-9 (1) **HIGH** CP-9 (1) (2) (3)								
CP-10 Information System Recovery and Reconstitution **LOW** CP-10 **MOD** CP-10 **HIGH** CP-10 (1)								
Effectiveness Level Reached								

NOTES:

7. Identification and Authentication *Class: Technical*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) identify information system users, processes acting on behalf of users, or devices; and (ii) authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Security Control	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Common Control**	**Compensating Control**	**Scoping Guidance Applied**
IA-1 Identification and Authentication Policy and Procedures **LOW** IA-1 **MOD** IA-1 **HIGH** IA-1								
IA-2 User Identification and Authentication **LOW** IA-2 **MOD** IA-2 **HIGH** IA-2 (1)								
IA-3 Device Identification and Authentication **LOW** Not Selected **MOD** IA-3 **HIGH** IA-3								
IA-4 Identifier Management **LOW** IA-4 **MOD** IA-4 **HIGH** IA-4								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
IA-5 Authenticator Management **LOW** IA-5 **MOD** IA-5 **HIGH** IA-5								
IA-6 Authenticator Feedback **LOW** IA-6 **MOD** IA-6 **HIGH** IA-6								
IA-7 Cryptographic Module Authentication **LOW** IA-7 **MOD** IA-7 **HIGH** IA-7								
Effectiveness Level Reached								

NOTES:

8. Incident Response *Class: Operational*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) establish an operational incident response capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
IR-1 Incident Response Policy and Procedures **LOW** IR-1 **MOD** IR-1 **HIGH** IR-1								
IR-2 Incident Response Training **LOW** Not Selected **MOD** IR-2 **HIGH** IR-2 (1) (2)								
IR-3 Incident Response Testing **LOW** Not Selected **MOD** IR-3 **HIGH** IR-3 (1)								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
IR-4 Incident Handling **LOW** IR-4 **MOD** IR-4 (1) **HIGH** IR-4 (1)								
IR-5 Incident Monitoring **LOW** Not Selected **MOD** IR-5 **HIGH** IR-5 (1)								
IR-6 Incident Reporting **LOW** IR-6 **MOD** IR-6 (1) **HIGH** IR-6 (1)								
IR-7 Incident Response Assistance **LOW** IR-7 **MOD** IR-7 (1) **HIGH** IR-7 (1)								
Effectiveness Level Reached								

NOTES:

9. Maintenance — *Class: Operational*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Security Control	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Common Control**	**Compensating Control**	**Scoping Guidance Applied**
MA-1 System Maintenance Policy and Procedures **LOW** MA-1 **MOD** MA-1 **HIGH** MA-1								
MA-2 Periodic Maintenance **LOW** MA-2 **MOD** MA-2 (1) **HIGH** MA-2 (1) (2)								
MA-3 Maintenance Tools **LOW** Not Selected **MOD** MA-3 **HIGH** MA-3 (1) (2) (3)								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
MA-4 Remote Maintenance **LOW** MA-4 **MOD** MA-4 **HIGH** MA-4 (1) (2) (3)								
MA-5 Maintenance Personnel **LOW** MA-5 **MOD** MA-5 **HIGH** MA-5								
MA-6 Timely Maintenance **LOW** Not Selected **MOD** MA-6 **HIGH** MA-6								
Effectiveness Level Reached								

NOTES:

10. Media Protection *Class: Operational*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) protect information contained in organizational information systems in printed form or on digital media; (ii) limit access to information in printed form or on digital media removed from organizational information systems to authorized users; and (iii) sanitize or destroy digital media before disposal or release for reuse.

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
MP-1 Media Protection Policy and Procedures **LOW** MP-1 **MOD** MP-1 **HIGH** MP-1								
MP-2 Media Access **LOW** MP2 **MOD** MP-2 **HIGH** MP-2 (1)								
MP-3 Media Labeling **LOW** Not Selected **MOD** MP-3 **HIGH** MP-3								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
MP-4 Media Storage **LOW** Not Selected **MOD** MP-4 **HIGH** MP-4								
MP-5 Media Transport **LOW** Not Selected **MOD** MP-5 **HIGH** MP-5								
MP-6 Media Sanitization **LOW** Not Selected **MOD** MP-6 **HIGH** MP-6								
MP-7 Media Destruction and Disposal **LOW** MP-7 **MOD** MP-7 **HIGH** MP-7								
Effectiveness Level Reached								

NOTES:

11. Physical and Environmental Protection *Class: Operational*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Security Control	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Common Control**	**Compensating Control**	**Scoping Guidance Applied**
PE-1 Physical and Environmental Protection Policy and Procedures **LOW** PD-1 **MOD** PE-1 **HIGH** PE-1							▨	▨
PE-2 Physical Access Authorizations **LOW** PE-2 **MOD** PE-2 **HIGH** PE-2	▨							
PE-3 Physical Access Control **LOW** PE-3 **MOD** PE-3 **HIGH** PE-3	▨							

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
PE-4 Access Control for Transmission Medium **LOW** Not Selected **MOD** Not Selected **HIGH** Not Selected								
PE-5 Access Control for Display Medium **LOW** Not Selected **MOD** PE-5 **HIGH** PE-5								
PE-6 Monitoring Physical Access **LOW** PE-6 **MOD** PE-6 (1) **HIGH** PE-6 (1) (2)								
PE-7 Visitor Control **LOW** PE-7 **MOD** PE-7 (1) **HIGH** PE-7 (1)								
PE-8 Access Logs **LOW** PE-8 **MOD** PE-8 (1) **HIGH** PE-8 (1)								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
PE-9 Power Equipment and Power Cabling **LOW** Not Selected **MOD** PE-9 **HIGH** PE-9								
PE-10 Emergency Shutoff **LOW** Not Selected **MOD** PE-10 **HIGH** PE-10								
PE-11 Emergency Power **LOW** Not Selected **MOD** PE-11 **HIGH** PE-11 (1)								
PE-12 Emergency Lighting **LOW** PE-12 **MOD** PE-12 **HIGH** PE-12								
PE-13 Fire Protection **LOW** PE-13 **MOD** PE-13 (1) **HIGH** PE-13 (1) (2)								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
PE-14 Temperature and Humidity Controls **LOW** PE-14 **MOD** PE-14 **HIGH** PE-14								
PE-15 Water Damage Protection **LOW** PE-15 **MOD** PE-15 **HIGH** PE-15 (1)								
PE-16 Delivery and Removal **LOW** PE-16 **MOD** PE-16 **HIGH** PE-16								
PE-17 Alternate Work Site **LOW** Not Selected **MOD** PE-17 **HIGH** PE-17								
Effectiveness Level Reached								

NOTES:

12. Planning *Class: Management*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

	L.1	L.2	L.3	L.4	L.5	Common	Compensating	Scoping Guidance Applied
Security Control	**Policy**	**Procedures**	**Implemented**	**Tested**	**Integrated**	**Control**	**Control**	
PL-1 Security Planning Policy and Procedures **LOW** PL-1 **MOD** PL1 **HIGH** PL-1								
PL-2 System Security Plan **LOW** PL-2 **MOD** PL-2 **HIGH** PL-2								
PL-3 System Security Plan Update **LOW** PL-3 **MOD** PL-3 **HIGH** PL-3								
PL-4 Rules of Behavior **LOW** PL-4 **MOD** PL-4 **HIGH** PL-4								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
PL-5 Privacy Impact Assessment **LOW** PL-5 | **MOD** PL-5 | **HIGH** PL-5								
Effectiveness Level Reached								

NOTES:

13. Personnel Security — *Class: Operational*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Security Control	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Common Control**	**Compensating Control**	**Scoping Guidance Applied**
PS-1 Personnel Security Policy and Procedures **LOW** PS-1 **MOD** PS-1 **HIGH** PS-1								
PS-2 Position Categorization **LOW** PS-2 **MOD** PS-2 **HIGH** PS-2								
PS-3 Personnel Screening **LOW** PS-3 **MOD** PS-3 **HIGH** PS-3								
PS-4 Personnel Termination **LOW** PS-4 **MOD** PS-4 **HIGH** PS-4								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
PS-5 Personnel Transfer **LOW** PS-5 **MOD** PS-5 **HIGH** PS-5								
PS-6 Access Agreements **LOW** PS-6 **MOD** PS-6 **HIGH** PS-6								
PS-7 Third-Party Personnel Security **LOW** PS-7 **MOD** PS-7 **HIGH** PS-7								
PS-8 Personnel Sanctions **LOW** PS-8 **MOD** PS-8 **HIGH** PS-8								
Effectiveness Level Reached								

NOTES:

14. Risk Assessment *Class: Management*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
RA-1 Risk Assessment Policy and Procedures **LOW** RA-1 **MOD** RA-1 **HIGH** RA-1								
RA-2 Security Categorization **LOW** RA-2 **MOD** RA-2 **HIGH** RA-2								
RA-3 Risk Assessment **LOW** RA-3 **MOD** RA-3 **HIGH** RA-3								
RA-4 Risk Assessment Update **LOW** RA-4 **MOD** RA-4 **HIGH** RA-4								

<table>
<tr><th>Security Control</th><th>L.1
Policy</th><th>L.2
Procedures</th><th>L.3
Implemented</th><th>L.4
Tested</th><th>L.5
Integrated</th><th>Common
Control</th><th>Compensating
Control</th><th>Scoping Guidance Applied</th></tr>
<tr><td><b>RA-5 Vulnerability Scanning</b>
<table>
<tr><td><b>LOW</b>
Not Selected</td><td><b>MOD</b>
RA-5</td><td><b>HIGH</b>
RA-5 (1) (2)</td></tr>
</table></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>Effectiveness Level Reached</b></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

NOTES:

15. System and Services Acquisition *Class: Management*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect outsourced organizational information, applications, and/or services.

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
SA-1 System and Services Acquisition Policy and Procedures **LOW** SA-1 **MOD** SA-1 **HIGH** SA-1								
SA-2 Allocation of Resources **LOW** SA-2 **MOD** SA-2 **HIGH** SA-2								
SA-3 Life Cycle Support **LOW** SA-3 **MOD** SA-3 **HIGH** SA-3								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
SA-4 Acquisitions **LOW** SA-4 **MOD** SA-4 **HIGH** SA-4								
SA-5 Information System Documentation **LOW** SA-5 **MOD** SA-5 (1) **HIGH** SA-5 (1) (2)								
SA-6 Software Usage Restrictions **LOW** SA-6 **MOD** SA-6 **HIGH** SA-6								
SA-7 User Installed Software **LOW** SA-7 **MOD** SA-7 **HIGH** SA-7								
SA-8 Security Design Principles **LOW** Not Selected **MOD** SA-8 **HIGH** SA-8								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
SA-9 Outsourced Information System Services **LOW** SA-9 **MOD** SA-9 **HIGH** SA-9								
SA-10 Developer Configuration Management **LOW** Not Selected **MOD** Not Selected **HIGH** SA-10								
SA-11 Developer Security Testing **LOW** Not Selected **MOD** SA-11 **HIGH** SA-11								
Effectiveness Level Reached								

NOTES:

16. System and Communications Protection *Class: Technical*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
SC-1 System and Communications Protection Policy and Procedures **LOW** SC-1 **MOD** SC-1 **HIGH** SC-1								
SC-2 Application Partitioning **LOW** Not Selected **MOD** SC-2 **HIGH** SC-2								
SC-3 Security Function Isolation **LOW** Not Selected **MOD** Not Selected **HIGH** SC-3								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
SC-4 Information Remnants **LOW** Not Selected **MOD** SC-4 **HIGH** SC-4								
SC-5 Denial of Service Protection **LOW** SC-5 **MOD** SC-5 **HIGH** SC-5								
SC-6 Resource Priority **LOW** Not Selected **MOD** SC-6 **HIGH** SC-6								
SC-7 Boundary Protection **LOW** SC-7 **MOD** SC-7 (1) **HIGH** SC-7 (1)								
SC-8 Transmission Integrity **LOW** Not Selected **MOD** SC-8 **HIGH** SC-8 (1)								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
SC-9 Transmission Confidentiality **LOW** Not Selected **MOD** SC-9 **HIGH** SC-9 (1)								
SC-10 Network Disconnect **LOW** Not Selected **MOD** SC-10 **HIGH** SC-10								
SC-11 Trusted Path **LOW** Not Selected **MOD** Not Selected **HIGH** Not Selected								
SC-12 Cryptographic Key Establishment and Management **LOW** Not Selected **MOD** SC-12 **HIGH** SC-12								
SC-13 Use of Validated Cryptography **LOW** SC-13 **MOD** SC-13 **HIGH** SC-13								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
SC-14 Public Access Protections **LOW** SC-14 **MOD** SC-14 **HIGH** SC-14								
SC-15 Collaborative Computing **LOW** Not Selected **MOD** SC-15 **HIGH** SC-15								
SC-16 Transmission of Security Parameters **LOW** Not Selected **MOD** Not Selected **HIGH** Not Selected								
SC-17 Public Key Infrastructure Certificates **LOW** Not Selected **MOD** SC-17 **HIGH** SC-17								
SC-18 Mobile Code **LOW** Not Selected **MOD** SC-18 **HIGH** SC-18								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
SC-19 Voice Over Internet Protocol **LOW** Not Selected **MOD** SC-19 **HIGH** SC-19								
Effectiveness Level Reached								

NOTES:

17. System and Information Integrity *Class: Operational*

FIPS 199 Impact Level: Low ___ Moderate ___ High ___

Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
SI-1 System and Information Integrity Policy and Procedures **LOW** SI-1 **MOD** SI-1 **HIGH** SI-1								
SI-2 Flaw Remediation **LOW** SI-2 **MOD** SI-2 **HIGH** SI-2								
SI-3 Malicious Code Protection **LOW** SI-3 **MOD** SI-3 (1) **HIGH** SI-3 (1) (2)								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
SI-4 Intrusion Detection Tools and Techniques **LOW** Not Selected **MOD** SI-4 **HIGH** SI-4								
SI-5 Security Alerts and Advisories **LOW** SI-5 **MOD** SI-5 **HIGH** SI-5								
SI-6 Security Functionality Verification **LOW** Not Selected **MOD** SI-6 **HIGH** SI-6 (1)								
SI-7 Software and Information Integrity **LOW** Not Selected **MOD** Not Selected **HIGH** SI-7								
SI-8 Spam and Spyware Protection **LOW** Not Selected **MOD** SI-8 **HIGH** SI-8 (1)								

Security Control	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Common Control	Compensating Control	Scoping Guidance Applied
SI-9 Information Input Restrictions **LOW** Not Selected **MOD** SI-9 **HIGH** SI-9								
SI-10 Information Input Accuracy, Completeness, and Validity **LOW** Not Selected **MOD** SI-10 **HIGH** SI-10								
SI-11 Error Handling **LOW** Not Selected **MOD** SI-11 **HIGH** SI-11								
SI-12 Information Output Handling and Retention **LOW** Not Selected **MOD** SI-12 **HIGH** SI-12								
Effectiveness Level Reached								

NOTES:

Appendix B
Information Security Program Assessment Questionnaire

Name of Agency Program: ______________________________

Name of Responsible Official: ______________________________

Name of Assessors: ______________________________

Date of Report: ______________________________

Time Period Covered in Report: ______________________________

Purpose of Report:

____

Agency Summary: **Number of systems in each FIPS 199 Impact Level Category**

Low: _______ Moderate: _______ High: _______

Part 1 –System Assessment Report Results

The answers to the following seventeen questions are derived from the results of the system assessments. The Level 1 (Policy) and Level 2 (Procedures) effectiveness levels are typically achieved through common security controls that are used by all systems. The answers to those two columns would be obtained at the agency level. It is recognized that there may be systems that have not reached the Level 3 (Implemented) and beyond for a specific control. To make the report more useful, it is recommended that the number of systems at the FIPS 199 impact levels be listed for the Level 3 through Level 5 effectiveness levels; then enter the percentage of systems that have reached that level for each control family at the FIPS 199 high-, moderate-, and low-impact levels.

Does the agency at the policy and procedures level and does every system at the implemented, tested, and integrated level meet the minimum controls in the following control families?	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**			**L.4 Tested**			**L.5 Integrated**			**Comments**
Insert # of systems at Low (L), Moderate (M), High (H) – FIPS 199 Impact Levels			**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**	
1. (AC) Access Control												

Does the agency at the policy and procedures level and does every system at the implemented, tested, and integrated level meet the minimum controls in the following control families?	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**			**L.4 Tested**			**L.5 Integrated**			**Comments**
Insert # of systems at Low (L), Moderate (M), High (H) – FIPS 199 Impact Levels			**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**	
2. (AT) Awareness and Training												
3. (AU) Audit and Accountability												
4. (CA) Certification, Accreditation, and Security Assessments												
5. (CM) Configuration Management												
6. (CP) Contingency Planning												

Does the agency at the policy and procedures level and does every system at the implemented, tested, and integrated level meet the minimum controls in the following control families?	L.1 Policy	L.2 Procedures	L.3 Implemented			L.4 Tested			L.5 Integrated			Comments
Insert # of systems at Low (L), Moderate (M), High (H) – FIPS 199 Impact Levels			L	M	H	L	M	H	L	M	H	
7. (IA) Identification and Authentication												
8. (IR) Incident Response												
9. (MA) System Maintenance												
10. (MP) Media Protection												

Does the agency at the policy and procedures level and does every system at the implemented, tested, and integrated level meet the minimum controls in the following control families?	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**			**L.4 Tested**			**L.5 Integrated**			**Comments**
Insert # of systems at Low (L), Moderate (M), High (H) – FIPS 199 Impact Levels			**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**	
11. (PE) Physical and Environmental Protection												
12. (PL) Security Planning												
13. (PS) Personnel Security												
14. (RA) Risk Assessment												
15. (SA) System and Services Acquisition												

Does the agency at the policy and procedures level and does every system at the implemented, tested, and integrated level meet the minimum controls in the following control families?	L.1 Policy	L.2 Procedures	L.3 Implemented			L.4 Tested			L.5 Integrated			Comments
Insert # of systems at Low (L), Moderate (M), High (H) – FIPS 199 Impact Levels			**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**	
16. (SC) System and Communications Protection												
17. (SI) System and Information Integrity												

Part 2 – Information Security Program Questions

In order to answer positively to each of the following program questions, the program activities/topic areas should be mentioned in high-level policy, and there should be documented procedures. The answers to the questions in this section are based on examining the procedures and program area documentation and interviewing key personnel to determine that the procedures are implemented.

Program Questions	Yes	No - Comments
1. Senior Agency Information Security Officer Has a senior agency information security officer been appointed with the mission and resources to develop and maintain an agency information security program?		
2. Security Control Review Process Does management ensure that corrective information security actions are tracked using the Plan-Of-Action & Milestones (POA&M) process?		
3. Capital Planning and Investment Control Does the agency require the use of a business case/Exhibit 300/Exhibit 53 to record the resources required for security at an acceptable level of risk for all programs and systems in the agency?		

Program Questions	Yes	No - Comments
4. Investment Review Board Is there an Investment Review Board (or similar group) designated and empowered to ensure that all investment requests include the security resources needed or that all exceptions to this requirement are documented?		
5. Integrating Information Security and Critical Infrastructure Protection into Capital Planning and Investment Control Is there integration of information security and Critical Infrastructure Protection (CIP) into the Capital Planning and Investment Control Process?		
6. Budget and Resources Are information security resources (internal FTEs and funding) allocated to protect information and information systems in accordance with assessed risks?		
7. Systems and Projects Inventory Are IT projects and systems identified in an inventory and is the information about the IT projects and systems relevant to the investment management process? Is there an inventory of systems as required by FISMA?		

Program Questions	Yes	No - Comments
8. IT Security Metrics Are IT security metrics collected agency-wide and reported to a central authority?		
9. Enterprise Architecture Is information security fully integrated into the agencies' enterprise architecture?		
10. Critical Infrastructure Protection Plan Is there a documented critical infrastructure and key resources protection plan that meets the requirements of HSPD-7?		

Appendix C
Glossary

Term	Definition
Acceptable Risk	A concern that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.
Access Control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances).
Access Control Lists (ACLs)	A register of: (1) users (including groups, machines, and processes) who have been given permission to use a particular system resource, and (2) the types of access they have been permitted.
Account Management, User	Involves (1) the process of requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Accreditation	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Accreditation Authority	See Authorizing Official.
Accreditation Boundary	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected.
Accreditation Package	The evidence provided to the authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to: (i) the system security plan; (ii) the assessment results from the security certification; and (iii) the plan of action and milestones.
Accrediting Authority	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Agency	See Executive Agency.

Term	Definition
Assessment Procedure	A set of activities or actions employed by an assessor to determine the extent to which a security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Asset	A major application, general support system, high-impact program, physical plant, mission-critical system, or a logically related group of systems.
Audit Trail	A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorize Processing	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Availability	Ensuring timely and reliable access to and use of information.
Awareness, Training, and Education	Includes (1) awareness programs set the stage for training by changing organizational attitudes toward realization of the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; and (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in automated information security.
Backup	A copy of files and programs made to facilitate recovery if necessary.
Biometric	A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and handwriting samples are all examples of biometrics.
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, 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.
Certification Agent	The individual, group, or organization responsible for conducting a security certification.

Term	Definition
Certification and Accreditation (C&A)	Certification involves the testing and evaluation of the technical and nontechnical security features of an IT system to determine its compliance with a set of specified security requirements. Accreditation is a process whereby a Designated Approval Authority (DAA) or other authorizing management official authorizes an IT system to operate for a specific purpose using a defined set of safeguards at an acceptable level of risk.
Chief Information Officer (CIO)	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Chief Information Security Officer	See Senior Agency Information Security Officer.
Clinger-Cohen Act of 1996	Also known as Information Technology Management Reform Act. A statute that substantially revised the way that federal IT resources are managed and procured, including a requirement that each agency design and implement a process for maximizing the value and assessing and managing the risks of IT investments.
Common Security Controls	Security controls that can be applied to one or more agency information systems and have the following properties: (i) the development, implementation, and assessment of the controls can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the controls can be used to support the security certification and accreditation processes of an agency information system where those controls have been applied.
Compensating Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high security control baselines that provide equivalent or comparable protection for an information system.
Computer Security Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.
Computer Security Incident Response Team (CSIRT)	A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).

Term	Definition
Computer Virus	A computer virus is similar to a Trojan horse because it is a program that contains hidden code, which usually performs some unwanted function as a side effect. The main difference between a virus and a Trojan horse is that the hidden code in a computer virus can only replicate by attaching a copy of itself to other programs and may also include an additional "payload" that triggers when specific conditions are met.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.
Contingency Plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system.
Denial of Service (DoS)	The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)
Designated Approving (Accrediting) Authority (DAA)	The individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.
Disaster Recovery Plan (DRP)	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
Distributed Denial of Service (DDoS)	A denial of service technique that uses numerous hosts to perform the attack.
Due Care	The responsibility that managers and their organizations have a duty to provide for information security to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed.
Electronic Signature	A method of signing an electronic message that -- (i) identifies and authenticates a particular person as the source of the electronic message; and (ii) indicates such person's approval of the information contained in the electronic message.
Encryption	Encryption is the conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people.
Executive Agency	An executive department specified in 5 United States Code (U.S.C.), Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

Term	Definition
Federal Information Processing Standard (FIPS)	A standard for adoption and use by federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.
Federal Information System	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
Firewall	A gateway that limits access between networks in accordance with local security policy.
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
High-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
Identification	The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.
Incident	An occurrence that actually or potentially jeopardizes 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.
Incident Response	The mitigation of violations of security policies and recommended practices.
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization’s IT system(s).
Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Term	Definition
Information System Owner	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Officer (ISSO)	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Interconnection Security Agreement (ISA)	An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a memorandum of understanding or agreement (MOU/A) between the organizations.
Intrusion Detection System (IDS)	Software that looks for suspicious activity and alerts administrators.
IT Security Architecture	A description of security principles and an overall approach for complying with the principles that drive the system design, i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments.
IT Security Metrics	Metrics based on information security performance goals and objectives.
Keystroke Monitoring	The process used to view or record both the keystrokes entered by a computer user and the computer’s response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.
Least Privilege	The security objective of granting users only those accesses they need to perform their official duties.

Term	Definition
Low-Impact System	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact of low.
Major Application	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.
Major Information System	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.
Malicious Code	A virus, worm, Trojan horse, or other code-based entity that infects a host.
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Media	Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Media Sanitization	The removal of information from a storage medium.
Metrics	Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.
Mission Critical	Any telecommunications or information system that is defined as a national security system (Federal Information Security Management Act of 2002 - FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.
Moderate-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
Password	A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources.

Term	Definition
Personal Identification Number (PIN)	A password consisting only of decimal digits.
Policy	A document that delineates the security management structure, clearly assigns security responsibilities, and lays the foundation necessary to reliably measure progress and compliance.
Potential Impact	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Privacy	Restricting access to subscriber or Relying Party information in accordance with federal law and agency policy.
Public Key	A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public; it is used to verify a digital signature; this key is mathematically linked with a corresponding private key.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Records	The recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results) which serve as the basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), organizational assets, or individuals that results from the operation of an information system given the potential impact of a threat and the likelihood of the occurrence of that threat.
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Risk Management	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
Risk Mitigation	Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

Term	Definition
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Rules of Behavior	The rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment and limitation of system privileges, and individual accountability.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.
Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
Scoping Guidance	Specific factors related to technology, infrastructure, public access, scalability, common security controls, and risk that can be considered by organizations in the applicability and implementation of individual security controls in the security control baseline.
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Control Baseline	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Goals	The five security goals are confidentiality, availability, integrity, accountability, and assurance.
Security Objective	Confidentiality, integrity, or availability.
Security Plan	See System Security Plan.
Security Policy	Security Policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities.

Term	Definition
Security Requirements	Requirements levied on an information system that are derived from applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.
Sensitive Information	Information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.
Sensitivity	Used in this guideline to mean a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.
Sensitivity Levels	A graduated system of marking (e.g., low, moderate, high) information and information processing systems based on threats and risks that result if a threat is successfully conducted.
Social Engineering	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge.
System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
System Administrator	A person who manages a multi-user computer system. Responsibilities are similar to that of a network administrator. A system administrator would perform systems programmer activities with regard to the operating system and other network control programs.
System Development Life Cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.
System Interconnection	The direct connection of two or more IT systems for the purpose of sharing data and other information resources.

Term	Definition
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Trojan Horse	A non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose.
Unauthorized Access	Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use.
User	Individual or (system) process authorized to access an information system.
Virus	A self-replicating program that runs and spreads by modifying other programs or files.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system.
Worm	A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Appendix D - References

Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003.

Federal Information Processing Standards Publication 200, Security Controls for Federal Information System, (projected for publication March 2005).

Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

National Institute of Standards and Technology Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998.

National Institute of Standards and Technology Special Publication 800-18, Revision 1, Guide for Developing Security Plans for Federal Information, (projected for publication fall 2005).

National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems, July 2002.

National Institute of Standards and Technology Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004.

National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems, February 2005.

National Institute of Standards and Technology Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, (projected for publication fall 2005).

Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, Management of Federal Information Resources, November 2000.