NIST Special Publication 800-26

Security Self-Assessment Guide for Information Technology Systems

Marianne Swanson

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

C O M P U T E R S E C U R I T Y

1901-2001
NIST CENTENNIAL

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
01SEP2001	N/A	-

Title and Subtitle Security Self-Assessment Guide for Information Technology Systems	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA 22102	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es) NIST	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms IATAC COLLECTION	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 99	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	9/1/2001	Report 9/1/2001

4. TITLE AND SUBTITLE
Security Self-Assessment Guide for Information Technology Systems

5. FUNDING NUMBERS

6. AUTHOR(S)
Marianne Swanson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

NIST

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

Adequate security of information and the systems that process it is a fundamental management responsibility. Agency officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

14. SUBJECT TERMS
IATAC Collection, information security

15. NUMBER OF PAGES
98

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

NIST Special Publication 800-26

Security Self-Assessment Guide for Information Technology Systems

Marianne Swanson

C O M P U T E R S E C U R I T Y

August 2001

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Karen H. Brown, Acting Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Karen H. Brown, Acting 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

Acknowledgements

Many people have contributed to this document, directly or indirectly. I would like to thank our NIST Technical Editor, Elizabeth Lennon, for spending a significant amount of her time editing this document. The questionnaire was field tested by Jim Craft, U.S. Agency for International Development, who provided a team to use the questionnaire on two systems. His team's input was invaluable in finalizing the document. I would also like to thank the many people who have provided comments on the draft and expressed their enthusiasm and support for the document. The development of the document was a consolidated effort by many people.

Executive Summary

Adequate security of information and the systems that process it is a fundamental management responsibility. Agency officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

Self-assessments provide a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. This self-assessment guide utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. The guide does not establish new security requirements. The control objectives and techniques are abstracted directly from long-standing requirements found in statute, policy, and guidance on security.

This document builds on the *Federal IT Security Assessment Framework* (Framework) developed by NIST for the Federal Chief Information Officer (CIO) Council. The Framework established the groundwork for standardizing on five levels of security status and criteria agencies could use to determine if the five levels were adequately implemented. This document provides guidance on applying the Framework by identifying 17 control areas, such as those pertaining to identification and authentication and contingency planning. In addition, the guide provides control objectives and techniques that can be measured for each area.

The questionnaire can be used for the following purposes:

- Agency managers who know their agency's systems and security controls can quickly gain a general understanding of needed security improvements for a system (major application or general support system), group of interconnected systems, or the entire agency.

- The security of an agency's system can be thoroughly evaluated using the questionnaire as a guide. The results of such a thorough review produce a reliable measure of security effectiveness and may be used to 1) fulfill reporting requirements; 2) prepare for audits; and 3) identify resources.

- The results of the questionnaire will assist, but not fulfill, agency budget requests as outlined in Office of Management and Budget (OMB) Circular A-11, "Preparing and Submitting Budget Estimates."

It is important to note that the questionnaire is not intended to be an all-inclusive list of control objectives and related techniques. Accordingly, it should be used in conjunction with the more detailed guidance listed in Appendix B. In addition, details associated with certain technical controls are not specifically provided due to their voluminous and dynamic nature. Agency managers should obtain information on such controls from other sources, such as vendors, and use that information to supplement this guide.

Consistent with OMB policy, each agency must implement and maintain a program to adequately secure its information and system assets. An agency program 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. Performing a self-assessment and mitigating any of the weaknesses found in the assessment is one way to determine if the system and the information are adequately secured.

Table of Contents

1. Introduction

A self-assessment conducted on a system (major application or general support system) or multiple self-assessments conducted for a group of interconnected systems (internal or external to the agency) is one method used to measure information technology (IT) security assurance. IT security assurance is the degree of confidence one has that the managerial, technical and operational security measures work as intended to protect the system and the information it processes. Adequate security of these assets is a fundamental management responsibility. Consistent with Office of Management and Budget (OMB) policy, each agency must implement and maintain a program to adequately secure its information and system assets. Agency 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 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 security programs and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

An important element of ensuring an organizations' IT security health is performing routine self-assessments of the agency security program. For a self-assessment to be effective, a risk assessment should be conducted in conjunction with or prior to the self-assessment. A self-assessment does not eliminate the need for a risk assessment.

There are many methods and tools for agency officials to help determine the current status of their security programs relative to existing policy. Ideally many of these methods and tools would be implemented on an ongoing basis to systematically identify programmatic weaknesses and where necessary, establish targets for continuing improvement. This document provides a method to evaluate the security of unclassified systems or groups of systems; it guides the reader in performing an IT security self-assessment. Additionally, the document provides guidance on utilizing the results of the system self-assessment to ascertain the status of the agency-wide security program. The results are obtained in a form that can readily be used to determine which of the five levels specified in the Federal IT Security Assessment Framework the agency has achieved for each topic area covered in the questionnaire. For example, the group of systems under review may have reached level 4 (Tested and Evaluated Procedures and Controls) in the topic area of physical and environmental protection, but only level 3 (Implemented Procedures and Controls) in the area of logical access controls.

1.1 Self -Assessments

This self-assessment guide utilizes an extensive questionnaire (Appendix A) containing specific control objectives and suggested techniques against which the security of a system or group of interconnected systems can be measured. The questionnaire can be based primarily on an examination of relevant documentation and a rigorous examination and test of the controls. This guide does not establish new security requirements. The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy. However the guide is not intended to be a comprehensive list of control objectives and related techniques. The guide should be used in conjunction with the more detailed guidance listed in Appendix B. In addition, specific technical controls, such as those related to individual technologies or vendors, are not specifically provided due to their volume and dynamic nature. It should also be noted that an agency might have additional laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability. Each agency should decide if additional security controls should be added to the questionnaire and, if so, customize the questionnaire appropriately.

The goal of this document is to provide a standardized approach to assessing a system. This document strives to blend the control objectives found in the many requirement and guidance documents. To assist the reader, a reference source is listed after each control objective question listed in the questionnaire. Specific attention was made to the control activities found in the General Accounting Office's (GAO) Federal Information System Control Audit Manual (FISCAM). FISCAM is the document GAO auditors and agency inspector generals use when auditing an agency. When FISCAM is referenced in the questionnaire, the major category initials along with the control activity number are provided, e.g., *FISCAM SP-3.1*. The cross mapping of the two documents will form a road map between the control objectives and techniques the audit community assess and the control objectives and techniques IT security program managers and program officials need to assess. The mapping provides a common point of reference for individuals fulfilling differing roles in the assessment process. The mapping ensures that both parties are reviewing the same types of controls.

The questionnaire may be used to assess the status of security controls for a system, an interconnected group of systems, or agency-wide. These systems include information, individual systems (e.g., major applications, general support systems, mission critical systems), or a logically related grouping of systems that support operational programs (e.g., Air Traffic Control, Medicare, Student Aid). Assessing all security controls and all interconnected system dependencies provides a metric of the IT security conditions of an agency. By using the procedures outlined in Chapter 4, the results of the assessment can be used as input on the status of an agency's IT security program.

1.2 Federal IT Security Assessment Framework

The Federal IT Security Assessment Framework issued by the federal Chief Information Officer Council in November 2000 provides a tool that agencies can use to routinely evaluate the status of their IT security programs. 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 Self-Assessment Guide builds on the Framework by providing questions on specific areas of control, such as those pertaining to access and service continuity, and a means of categorizing evaluation results in the same manner as the Framework. See Appendix C for a copy of the Framework.

1.3 Audience

The control objectives and techniques presented 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 IT security at the system level and organization level. Additionally, internal and external auditors may use the questionnaire to guide their review of the IT security of systems. To perform the examination and testing required to complete the questionnaire, the assessor must be familiar with and able to apply a core knowledge set of IT security basics needed to protect information and systems. In some cases, especially in the area of examining and testing technical controls, assessors with specialized technical expertise will be needed to ensure that the questionnaire's answers are reliable.

1.4 Structure of this Document

Chapter 1 introduces the document and explains IT security assessments and the relationship to other documents. Chapter 2 provides a method for determining the system boundaries and criticality of the data. Chapter 3 describes the questionnaire. Chapter 4 provides guidance on using the completed system questionnaire(s) as input into obtaining an assessment of an agency-wide IT security program. Appendix A contains the questionnaire. Appendix B lists the documents used in compiling the assessment control objective questions. Appendix C contains a copy of the *Federal IT Security Assessment Framework*. Appendix D lists references used in developing this document.

2. System Analysis

The questionnaire is a tool for completing an internal assessment of the controls in place for a major application or a general support system. The security of every system or group of interconnected system(s) must be described in a security plan. The system may consist of a major application or be part of a general support system. The definition of major application and general support system are contained in Appendix C. Before the questionnaire can be used effectively, a determination must be made as to the boundaries of the system and the sensitivity and criticality 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 and the criticality level of the data. If a plan has not been prepared for the system, the completion of this self-assessment will aid in developing the system security plan. Many of the control objectives addressed in the assessment are to be described in the system security plan. The following two sections, Section 2.1 and Section 2.2, contain excerpts from NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems,* and will assist the reader in determining the physical and logical boundaries of the system and the criticality of the information.

2.1 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, *Guide for Developing Security Plans for Information Technology Systems,* is identified by defining boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a system security plan and a security evaluation whenever a major modification to the system occurs. Each element of the system must[1]:

- Be under the **same** direct management control;
- Have the **same** function or mission objective;
- Have essentially the **same** operating characteristics and security needs; and
- Reside in the **same** general operating environment.

[1] OMB Circular A-130, Appendix III defines general support system or "system" in similar terms.

All components of a system need not be physically connected (e.g., [1] a group of stand-alone personal computers (PCs) in an office; [2] a group of PCs placed in employees' homes under defined telecommuting program rules; [3] a group of portable PCs provided to employees who require mobile computing capability to perform their jobs; and [4] a system with multiple identical configurations that are installed in locations with the same environmental and physical controls).

An important element of the assessment will be determining the effectiveness of the boundary controls when the 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 controls related to each system that is connected to the system under review.

2.2 Sensitivity Assessment

Effective use of the questionnaire presumes a comprehensive understanding of the value of the systems and information being assessed. Value can be expressed in terms of the degree of sensitivity or criticality of the systems and information relative to each of the five protection categories in section 3534(a)(1)(A) of the Government Information Security Reform provisions of the National Defense Authorization Act of 2000, i.e., integrity, confidentiality, availability, authenticity, and non-repudiation. The addition of authenticity and non-repudiation as protection categories within the Reform Act was to stress the need for these assurances as the government progresses towards a paperless workplace. There are differing opinions on what constitutes protection categories, for continuity within several NIST Special Publication 800 documents; authenticity, non-repudiation, and accountability are associated with the integrity of the information.

- ***Confidentiality*** - The information requires protection from unauthorized disclosure.

- ***Integrity*** - The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to:
    - *Authenticity* – A third party must be able to verify that the content of a message has not been changed in transit.
    - *Non-repudiation* – The origin or the receipt of a specific message must be verifiable by a third party.
    - *Accountability* - A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

- ***Availability*** - The information technology resource (system or data) must be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes.

When determining the value, consider any laws, regulations, or policies that establish specific requirements for integrity, confidentiality, authenticity, availability, and non-repudiation of data and information in the system. Examples might include Presidential Decision Directive 63, the Privacy Act, or a specific statute or regulation concerning the information processed (e.g., tax or census information).

Consider the information processed by the system and the need for protective measures. Relate the information processed to each of the three basic protection requirements above (**confidentiality**, **integrity**, and **availability).** In addition, it is helpful to categorize the system or group of systems by sensitivity level. Three examples of such categories for sensitive unclassified information are described below:

- *High* — Extremely grave injury accrues to U.S. interests if the information is compromised; could cause loss of life, imprisonment, major financial loss, or require legal action for correction

- *Medium*—Serious injury accrues to U.S. interests if the information is compromised; could cause significant financial loss or require legal action for correction

- *Low* —Injury accrues to U.S. interests if the information is compromised; would cause only minor financial loss or require only administrative action for correction

For example, a system and its information may require a high degree of integrity and availability, yet have no need for confidentiality.

Many agencies have developed their own methods of making these determinations. Regardless of the method used, the system owner/program official is responsible for determining the sensitivity of the system and information. The sensitivity should be considered as each control objective question in the questionnaire is answered. When a determination is made to either provide more rigid controls than are addressed by the questionnaire or not to implement the control either temporarily or permanently, there is a risk based decision field in the questionnaire that can be checked to indicate that a determination was made. The determination for lesser or more stringent protection should be made due to either the sensitivity of the data and operations affected or because there are compensating controls that lessen the need for this particular control technique. It should be noted in the comments section of the questionnaire that the system security plan contains supporting documentation as to why the specific control has or has not been implemented.

3. Questionnaire Structure

The self-assessment questionnaire contains three sections: cover sheet, questions, and notes. The questionnaire begins with a cover sheet requiring descriptive information about the major application, general support system, or group of interconnected systems being assessed. The questionnaire provides a hierarchical approach to assessing a system by containing critical elements and subordinate questions. The critical element level should be determined based on the answers to the subordinate questions. The critical elements are derived primarily from OMB Circular A-130. The subordinate questions address the control objectives and techniques that can be implemented to meet the critical elements. Assessors will need to carefully review the levels of subordinate control objectives and techniques in order to determine what level has been reached for the related critical element. The control objectives were obtained from the list of source documents located in Appendix B. There is flexibility in implementing the control objectives and techniques. It is feasible that not all control objectives and techniques may be needed to achieve the critical element.

The questionnaire section may be customized by the organization. An organization can add questions, require more descriptive information, and even pre-mark certain questions if applicable. For example, many agencies may have personnel security procedures that apply to all systems within the agency. The level 1 and level 2 columns in the questionnaire can be pre-marked to reflect the standard personnel procedures in place. Additional columns may be added to reflect the status of the control, i.e., planned action date, non-applicable, or location of documentation. The questionnaire should not have questions removed or questions modified to reduce the effectiveness of the control.

After each question, there is a comment field and an initial field. The comment field can be used to note the reference to supporting documentation that is attached to the questionnaire or is obtainable for that question. The initial field can be used when a risk based decision is made concerning not to implement a control or if the control is not applicable for the system. At the end of each set of questions, 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 control objective is not being implemented fully 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 section may reference supporting documentation on how the control objectives and techniques were tested and a summary of findings.

3.1 Questionnaire Cover Sheet

This section provides instruction on completing the questionnaire cover sheet, standardizing on how the completed evaluation should be marked, how systems are titled, and labeling the criticality of the system.

3.1.1 Questionnaire Control

All completed questionnaires should be marked, handled, and controlled at the level of sensitivity determined by organizational policy. It should be noted that the information contained in a completed questionnaire could easily depict where the system or group of systems is most vulnerable.

3.1.2 System Identification

The cover page of the questionnaire begins with the name and title of the system to be evaluated. As explained in NIST Special Publication 800-18, 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 requirements are met based on the unique requirements for the system, and that allocated resources are appropriately applied. Further, the use of unique system identifiers is integral to the IT system investment models and analyses established under the requirements of the Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act). The identifiers are required by OMB Circular A-11 and used in the annual OMB budget submissions of the Exhibit 53 and 300. In light of OMB policies concerning capital planning and investment control, the unique name/identifier should remain the same throughout the life of the system to allow the organization to track completion of security requirements over time. Please see OMB Circular A-11, Section 53.7 for additional information on assigning unique identifiers. If no unique name/identifier has been assigned or is not known, contact the information resource management office for assistance.

In many cases the major application or general support system will contain interconnected systems. The connected systems should be listed and once the assessment is complete, a determination should be made and noted on the cover sheet as to whether the boundary controls are effective. The boundary controls should be part of the assessment. If the boundary controls are not adequate, the connected systems should be assessed as well.

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.

3.1.3 Purpose and Assessor Information

The purpose and objectives of the assessment should be identified. For example, the assessment is intended to gain a high-level indication of system security in preparation for a more detailed review or the assessment is intended to be a thorough and reliable

evaluation for purposes of developing an action plan. The name, title, and organization 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 evaluation will vary. The time and resources needed to complete the assessment will vary depending on the size and complexity of the system, accessibility of system and user data, and how much information is readily available for the assessors to evaluate. For example, if a system has undergone extensive testing, certification, and documentation, the self-assessment is easy to use and serves as a baseline for future evaluations. If the system has undergone very limited amounts of testing and has poor documentation, completing the questionnaire will require more time.

3.1.4 Criticality of Information

The level of sensitivity of information as determined by the program official or system owner should be documented using the table on the questionnaire cover sheet. If an organization has designed their own method of determining system criticality or sensitivity, the table should be replaced with the organization's criticality or sensitivity categories. The premise behind formulating the level of sensitivity is that systems supporting higher risk operations would be expected to have more stringent controls than those that support lower risk operations.

3.2 Questions

The questions are separated into three major control areas: 1) management controls, 2) operational controls, and 3) technical controls. The division of control areas in this manner complements three other NIST Special Publications: NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook* (Handbook), NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* (Principles and Practices), and NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems* (Planning Guide). All three documents should be referenced for further information. The Handbook should be used to obtain additional detail for any of the questions (control objectives) listed in the questionnaire. The Principles and Practices document should be used as a reference to describe the security controls. The Planning Guide formed the basis for the questions listed in the questionnaire. The documents can be obtained from the NIST Computer Security Resource Center web site at the URL: http://csrc.nist.gov.

The questions portion of this document easily maps to the three NIST documents described above since the chapters in all three documents are organized by the same control areas, i.e., management, operational, and technical.

Within each of the three control areas, there are a number of topics; for example, personnel security, contingency planning, and incident response are topics found under the operational control area. There are a total of 17 topics contained in the questionnaire; each topic contains critical elements and supporting security control objectives and techniques (questions) about the system. The critical elements are derived primarily from OMB Circular A-130 and are integral to an effective IT security program. The control objectives and techniques support the critical elements. If a number of the control objectives and techniques are not implemented, the critical elements have not been met.

Each control objective and technique may or may not be implemented depending on the system and the risk associated with the system. Under each control objective and technique question, one or more of the source documents is referenced. The reference points to the specific control activity in the GAO FISCAM document or to the title of any of the other documents listed in Appendix B, Source of Control Criteria.

Management Controls

1. Risk Management
2. Review of Security Controls
3. Life Cycle
4. Authorize Processing (Certification and Accreditation)
5. System Security Plan

Operational Controls

6. Personnel Security
7. Physical Security
8. Production, Input/Output Controls
9. Contingency Planning
10. Hardware and Systems Software Maintenance
11. Data Integrity
12. Documentation
13. Security Awareness, Training, and Education
14. Incident Response Capability

Technical Controls

15. Identification and Authentication
16. Logical Access Controls
17. Audit Trails

Figure 1. Topic Areas

In order to measure the progress of effectively implementing the needed security control, five levels of effectiveness are provided for each answer to the security control question:

- Level 1 – control objective documented in a security policy
- Level 2 – security controls documented as procedures
- Level 3 – procedures have been implemented
- Level 4 – procedures and security controls are tested and reviewed
- Level 5 – procedures and security controls are fully integrated into a comprehensive program.

The method for answering the questions can be based primarily on an examination of relevant documentation and a rigorous examination and test of the controls. The review, for example, should consist of testing the access control methods in place by performing a penetration test; examining system documentation such as software change requests forms, test plans, and approvals; and examining security logs and audit trails. 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 checklist, including all references, is completed for the first time, future assessments of the system will require considerably less effort. The completed questionnaire would establish a baseline. If this year's assessment indicates that most of the controls in place are at level 2 or level 3, then that would be the starting point for the next evaluation. 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 comment section to list whether there is supporting documentation and the notes section for any lengthy explanations.

The audit techniques to test the implementation or effectiveness of each control objective and technique are beyond the scope of this document. The GAO FISCAM document provides audit techniques that can be used to test the control objectives.

When answering the questions about whether a specific control objective has been met, consider the sensitivity of the system. The questionnaire contains a field that can be checked when a risk-based decision has been made to either reduce or enhance a security control. There may be certain situations where management will grant a waiver either because compensating controls exists or because the benefits of operating without the control (at least temporarily) outweigh the risk of waiting for full control implementation. Alternatively, there may be times when management implements more stringent controls than generally applied elsewhere. When the risk-based decision field is checked, note the reason in the comment field of the questionnaire and have management review and initial the decision. Additionally, the system security plan for the system should contain supporting documentation as to why the control has or has not been implemented.

The assessor must read each control objective and technique question and determine in partnership with the system owner and those responsible for administering the system, whether the system's sensitivity level warrants the implementation of the control stated in the question. If the control is applicable, check 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 shaded fields in the questionnaire do not require a check mark. The five levels describing the state of the control objective provide a picture of each operational control; however, how well each one of these controls is met is subjective. Criteria have been established for each of the five levels that should be applied when determining whether the control objective has fully reached one or more of the five levels. The criteria are contained in Appendix C, *Federal IT Security Assessment Framework.*

Based on the responses to the control objectives and techniques and in partnership with the system owner and those responsible for system administration, the assessor should conclude the level of the related critical element. The conclusion should consider the relative importance of each subordinate objective/technique to achieving the critical element and the rigor with which the technique is implemented, enforced, and tested.

3.3 Applicability of Control Objectives

As stated above, the critical elements are required to be implemented; the control objectives and techniques, however, tend to be more detailed and leave room for reasonable subjective decisions. If the control does not reasonably apply to the system, then a "non-applicable" or "N/A" can be entered next to the question.

The control objectives and techniques in the questionnaire are geared for a system or group of connected systems. It is possible to use the questionnaire for a program review at an organizational level for ascertaining if the organization has policy and procedures in place (level 1 or level 2). However, to ensure all systems have implemented, tested and fully integrated the controls (level 3, level 4, and level 5), the assessment questionnaire must be applied to each individual or interconnected group of systems. Chapter 4 describes how the results of the assessment can be used as input into an IT security program review.

The policy and procedures for a control objective and technique can be found at the Department level, agency level, agency component level, or application level. To effectively assess a system, ensure that the control objectives being assessed are at the applicable level. For example, if the system being reviewed has stringent authentication procedures, the authentication procedures for the system should be assessed, instead of the agency-wide minimum authentication procedures found in the agency IT security manual.

If a topic area is documented at a high level in policy, the level 1 box should be checked in the questionnaire. If there are additional low level policies for the system, describe the policies in the comment section of the questionnaire. If a specific control is described in detail in procedures, and implemented, the level 2 and level 3 boxes should be checked in the questionnaire. Testing and reviewing controls are an essential part of securing a system. For each specific control, check whether it has been tested and/or reviewed when a significant change occurred. The goal is to have all levels checked for each control. A conceptual sample of completing the questionnaire is contained in Appendix C. The conceptual sample has evolved into the questionnaire and differs slightly, i.e., there is now a comment and initial field.

4. Utilizing the Completed Questionnaire

The questionnaire can be used for two purposes. First it can be used by agency managers who know their agency's systems and security controls to quickly gain a general understanding of where security for a system, group of systems, or the entire agency needs improvement. 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 reporting requirements; 2) prepare for audits; and 3) identify resource needs.

4.1 Questionnaire Analysis

Because this is a self-assessment, ideally the individuals assessing the system are the owners of the system or responsible for operating or administering the system. The same individuals who completed the assessment can conduct the analysis of the completed questionnaire. By being familiar with the system, the supporting documentation, and the results of the assessment, the next step that the assessor takes is an analysis, which summarizes the findings. A centralized group, such as an agency's Information System Security Program Office, can also conduct the analysis as long as the supporting documentation is sufficient. The results of the analysis should be placed in an action plan, and the system security plan should be created or updated to reflect each control objective and technique decision.

4.2 Action Plans

How the critical element is to be implemented, i.e., specific procedures written, equipment installed and tested, and personnel trained, should be documented in an action plan. The action plan must contain projected dates, an allocation of resources, and follow-up reviews to ensure that remedial actions have been effective. Routine reports should be submitted to senior management on weaknesses identified, the status of the action plans, and the resources needed.

4.3 Agency IT Security Program Reports

Over the years, agencies have been asked to report on the status of their IT security program. The reporting requests vary in how much detail is required and in the type of information that should be reported. The completed self-assessment questionnaires are a useful resource for compiling agency reports. Below are sample topics that should be considered in an agency-wide security program report:

- Security Program Management
- Management Controls

- Operational Controls
- Technical Controls
- Planned Activities

4.3.1 Security Program Management

An agency's IT security program report needs to address programmatic issues such as:

- an established agency-wide security management structure,
- a documented up-to-date IT security program plan or policy *(The assessment results for level 1 provides input.)*
    - an agency-developed risk management and mitigation plan,
    - an agency-wide incident response capability,
    - an established certification and accreditation policy,
    - an agency-wide anti-virus infrastructure in place and operational at all agency facilities,
    - information security training and awareness programs established and available to all agency employees,
    - roles and relationships clearly defined and established between the agency and bureau levels of information security program management,
- an understanding of the importance of protecting mission critical information assets,
- the integration of security into the capital planning process,
- methods used to ensure that security is an integral part of the enterprise architecture (*The assessment results for the Life Cycle topic area provides input.),*
- the total security cost from this year's budget request and a breakdown of security costs by each major operating division, and
- descriptions of agency-wide guidance issued in the past year.

4.3.2 Management Controls, Operational Controls, and Technical Controls

The results of the completed questionnaires' 17 control topic areas can be used to summarize an agency's implementation of the management, operational, and technical controls. For the report to project an accurate picture, the results must be summarized by system type, not totaled into an overall agency grade level. For example, ten systems were assessed using the questionnaire. Five of the ten systems assessed were major applications; the other five were general support systems. The summary would separate the systems into general support systems and major applications.

By further separating them into groups according to criticality, the report stresses which systems and which control objectives require more attention based on sensitivity and criticality. Not all systems require the same level of protection; the report should reflect that diversity. The use of percentages for describing compliance (i.e., 50 percent of the major applications and 25 percent of general support systems that are high in criticality have complete and current system security plans within the past three years) can be used as long as there is a distinct division provided between the types of systems being reported.

Additionally all or a sampling of the completed questionnaires can be analyzed to determine which controls if implemented would impact the most systems. For example, if viruses frequently plague systems, a stricter firewall policy that prevents attached files in E-mail may be a solution. Also, systemic problems should be culled out. If an agency sees an influx of poor password management controls in the questionnaire results, then possibly password checkers should be used, awareness material issued, and password-aging software installed.

The report should conclude with a summary of planned IT security initiatives. The summary should include goals, actions needed to meet the goals, projected resources, and anticipated dates of completion.

Appendix A

System Questionnaire

System Name, Title, and Unique Identifier: _____

Major Application _____ or General Support System _____

Name of Assessors: _____
_____
_____

Date of Evaluation: _____

List of Connected Systems:

Name of System	Are boundary controls effective?	Planned action if not effective
1.		
2.		
3.		

Criticality of System	Category of Sensitivity High, Medium, or Low
Confidentiality	
Integrity	
Availability	

Purpose and Objective of Assessment: _____

_____

_____

Management Controls

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

1. Risk Management

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Risk Management *OMB Circular A-130, III*								
1.1 Critical Element: Is risk periodically assessed?								
1.1.1 Is the current system configuration documented, including links to other systems? *NIST SP 800-18*								
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? *FISCAM SP-1*								
1.1.3 Has data sensitivity and integrity of the data been considered? *FISCAM SP-1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.1.4 Have threat sources, both natural and manmade, been identified? *FISCAM SP-1*								
1.1.5 Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current? *NIST SP 800-30*[2]								
1.1.6 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities? *NIST SP 800-30*								
1.2. Critical Element: Do program officials understand the risk to systems under their control and determine the acceptable level of risk?								
1.2.1 Are final risk determinations and related management approvals documented and maintained on file? *FISCAM SP-1*								
1.2.2 Has a mission/business impact analysis been conducted? *NIST SP 800-30*								
1.2.3 Have additional controls been identified to sufficiently mitigate identified risks? *NIST SP 800-30*								

[2] Draft NIST Special Publication 800-30, "Risk Management Guidance" dated June 2001.

NOTES:

2. Review of Security Controls

Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Review of Security Controls *OMB Circular A-130, III* *FISCAM SP-5* *NIST SP 800-18*								
2.1. Critical Element: **Have the security controls of the system and interconnected systems been reviewed?**								
2.1 1 Has the system and all network boundaries been subjected to periodic reviews? *FISCAM SP-5.1*								
2.1.2 Has an independent review been performed when a significant change occurred? *OMB Circular A-130, III* *FISCAM SP-5.1* *NIST SP 800-18*								
2.1.3 Are routine self-assessments conducted ? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing? *OMB Circular A-130, 8B3* *NIST SP 800-18*								
2.1.5 Are security alerts and security incidents analyzed and remedial actions taken? *FISCAM SP 3-4* *NIST SP 800-18*								
2.2. Critical Element: **Does management ensure that corrective actions are effectively implemented?**								
2.2.1 Is there an effective and timely process for reporting significant weakness and ensuring effective remedial action? *FISCAM SP 5-1 and 5.2* *NIST SP 800-18*								

NOTES:

3. Life Cycle

Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Life Cycle *OMB Circular A-130, III* *FISCAM CC-1.1*								
3.1. Critical Element: **Has a system development life cycle methodology been developed?**								
Initiation Phase								
3.1.1 Is the sensitivity of the system determined? *OMB Circular A-130, III* *FISCAM AC-1.1 & 1.2* *NIST SP 800-18*								
3.1.2 Does the business case document the resources required for adequately securing the system? *Clinger-Cohen*								
3.1.3 Does the Investment Review Board ensure any investment request includes the security resources needed? *Clinger-Cohen*								
3.1.4 Are authorizations for software modifications documented and maintained? *FISCAM CC –1.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.5 Does the budget request include the security resources required for the system? *GISRA*								
Development/Acquisition Phase								
3.1.6 During the system design, are security requirements identified? *NIST SP 800-18*								
3.1.7 Was an initial risk assessment performed to determine security requirements? *NIST SP 800-30*								
3.1.8 Is there a written agreement with program officials on the security controls employed and residual risk? *NIST SP 800-18*								
3.1.9 Are security controls consistent with and an integral part of the IT architecture of the agency? *OMB Circular A-130, 8B3*								
3.1.10 Are the appropriate security controls with associated evaluation and test procedures developed before the procurement action? *NIST SP 800-18*								
3.1.11 Do the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.12 Do the requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented? *NIST SP 800-18*								
Implementation Phase								
3.2. Critical Element: Are changes controlled as programs progress through testing to final approval?								
3.2.1 Are design reviews and system tests run prior to placing the system in production? *FISCAM CC-2.1* *NIST SP 800-18*								
3.2.2 Are the test results documented? *FISCAM CC-2.1* *NIST SP 800-18*								
3.2.3 Is certification testing of security controls conducted and documented? *NIST SP 800-18*								
3.2.4 If security controls were added since development, has the system documentation been modified to include them? *NIST SP 800-18*								
3.2.5 If security controls were added since development, have the security controls been tested and the system recertified? *FISCAM CC-2.1* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.6 Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards? *NIST SP 800-18*								
3.2.7 Does the system have written authorization to operate either on an interim basis with planned corrective action or full authorization? *NIST SP 800-18*								
Operation/Maintenance Phase								
3.2.8 Has a system security plan been developed and approved? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*								
3.2.9 If the system connects to other systems, have controls been established and disseminated to the owners of the interconnected systems? *NIST SP 800-18*								
3.2.10 Is the system security plan kept current? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*								
Disposal Phase								
3.2.11 Are official electronic records properly disposed/archived? NIST SP 800-18								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere? *FISCAM AC-3.4* *NIST SP 800-18*								
3.2.13 Is a record kept of who implemented the disposal actions and verified that the information or media was sanitized? *NIST SP 800-18*								

NOTES:

4. Authorize Processing (Certification & Accreditation)

Authorize processing (Note: Some agencies refer to this process as certification and accreditation) provides a form of assurance of the security of the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Authorize Processing (Certification & Accreditation) *OMB Circular A-130, III* *FIPS 102*								
4.1. Critical Element: **Has the system been certified/recertified and authorized to process (accredited)?**								
4.1.1 Has a technical and/or security evaluation been completed or conducted when a significant change occurred? *NIST SP 800-18*								
4.1.2 Has a risk assessment been conducted when a significant change occurred? *NIST SP 800-18*								
4.1.3 Have Rules of Behavior been established and signed by users? *NIST SP 800-18*								
4.1.4 Has a contingency plan been developed and tested? *NIST SP 800-18*								
4.1.5 Has a system security plan been developed, updated, and reviewed? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
4.1.6 Are in-place controls operating as intended? *NIST SP 800-18*								
4.1.7 Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity? *NIST SP 800-18*								
4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization or contractor)? *NIST 800-18*								
4.2. Critical Element: Is the system operating on an interim authority to process in accordance with specified agency procedures?								
4.2.1 Has management initiated prompt action to correct deficiencies? *NIST SP 800-18*								

NOTES:

5. System Security Plan

System security plans provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
System security plan *OMB Circular A-130, III* *NIST SP 800-18* *FISCAM SP-2.1*								
5.1. Critical Element: **Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?**								
5.1.1 Is the system security plan approved by key affected parties and management? *FISCAM SP-2.1* *NIST SP 800-18*								
5.1.2 Does the plan contain the topics prescribed in NIST Special Publication 800-18? *NIST SP 800-18*								
5.1.3 Is a summary of the plan incorporated into the strategic IRM plan? *OMB Circular A-130, III* *NIST SP 800-18*								
5.2. Critical Element: **Is the plan kept current?**								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
5.2.1 Is the plan reviewed periodically and adjusted to reflect current conditions and risks? *FISCAM SP-2.1* *NIST SP 800-18*								

NOTES:

Operational Controls

The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

6. Personnel Security

Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Personnel Security *OMB Circular A-130, III*								
6.1. Critical Element: **Are duties separated to ensure least privilege and individual accountability?**								
6.1.1 Are all positions reviewed for sensitivity level? *FISCAM SD-1.2* *NIST SP 800-18*								
6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties? *FISCAM SD-1.2*								

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.1.3 Are sensitive functions divided among different individuals? *OMB Circular A-130, III* *FISCAM SD-1* *NIST SP 800-18*								
6.1.4 Are distinct systems support functions performed by different individuals? *FISCAM SD-1.1*								
6.1.5 Are mechanisms in place for holding users responsible for their actions? *OMB Circular A-130, III* *FISCAM SD-2 & 3.2*								
6.1.6 Are regularly scheduled vacations and periodic job/shift rotations required? *FISCAM SD-1.1* *FISCAM SP-4.1*								
6.1.7 Are hiring, transfer, and termination procedures established? *FISCAM SP-4.1* *NIST SP 800-18*								
6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts? *FISCAM SP-4.1* *NIST 800-18*								
6.2. Critical Element: **Is appropriate background screening for assigned positions completed prior to granting access?**								

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter? *OMB Circular A-130, III* *FISCAM SP-4.1*								
6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information? *FISCAM SP-4.1*								
6.2.3 When controls cannot adequately protect the information, are individuals screened prior to access? *OMB Circular A-130, III*								
6.2.4 Are there conditions for allowing system access prior to completion of screening? *FISCAM AC-2.2* *NIST SP 800-18*								

NOTES:

7. Physical and Environmental Protection

Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Physical and Environmental Protection								
Physical Access Control								
7.1. Critical Element: Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?								
7.1.1 Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics? *FISCAM AC-3 NIST SP 800-18*								
7.1.2 Does management regularly review the list of persons with physical access to sensitive facilities? *FISCAM AC-3.1*								
7.1.3 Are deposits and withdrawals of tapes and other storage media from the library authorized and logged? *FISCAM AC-3.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.4 Are keys or other access devices needed to enter the computer room and tape/media library? *FISCAM AC-3.1*								
7.1.5 Are unused keys or other entry devices secured? *FISCAM AC-3.1*								
7.1.6 Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc? *FISCAM AC-3.1*								
7.1.7 Are visitors to sensitive areas signed in and escorted? *FISCAM AC-3.1*								
7.1.8 Are entry codes changed periodically? *FISCAM AC-3.1*								
7.1.9 Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken? *FISCAM AC-4*								
7.1.10 Is suspicious access activity investigated and appropriate action taken? *FISCAM AC-4.3*								
7.1.11 Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks? *FISCAM AC-3.1*								
Fire Safety Factors								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.12 Are appropriate fire suppression and prevention devices installed and working? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.13 Are fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, reviewed periodically? *NIST SP 800-18*								
Supporting Utilities								
7.1.14 Are heating and air-conditioning systems regularly maintained? *NIST SP 800-18*								
7.1.15 Is there a redundant air-cooling system? *FISCAM SC-2.2*								
7.1.16 Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.17 Are building plumbing lines known and do not endanger system? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.18 Has an uninterruptible power supply or backup generator been provided? *FISCAM SC-2.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.19 Have controls been implemented to mitigate other disasters, such as floods, earthquakes, etc.? *FISCAM SC-2.2*								
Interception of Data								
7.2. Critical Element: Is data protected from interception?								
7.2.1 Are computer monitors located to eliminate viewing by unauthorized persons? *NIST SP 800-18*								
7.2.2 Is physical access to data transmission lines controlled? *NIST SP 800-18*								
Mobile and Portable Systems								
7.3. Critical Element: Are mobile and portable systems protected?								
7.3.1 Are sensitive data files encrypted on all portable systems? *NIST SP 800-14*								
7.3.2 Are portable systems stored securely? *NIST SP 800-14*								

NOTES:

8. Production, Input/Output Controls

There are many aspects to supporting IT operations. Topics range from a user help desk to procedures for storing, handling and destroying media. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Production, Input/Output Controls								
8.1. Critical Element: Is there user support?								
8.1.1 Is there a help desk or group that offers advice? *NIST SP 800-18*								
8.2. Critical Element: Are there media controls?								
8.2.1 Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information? *NIST SP 800-18*								
8.2.2 Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media? *NIST SP 800-18*								
8.2.3 Are audit trails used for receipt of sensitive inputs/outputs? *NIST SP 800-18*								
8.2.4 Are controls in place for transporting or mailing media or printed output? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
8.2.5 Is there internal/external labeling for sensitivity? *NIST SP 800-18*								
8.2.6 Is there external labeling with special handling instructions? *NIST SP 800-18*								
8.2.7 Are audit trails kept for inventory management? *NIST SP 800-18*								
8.2.8 Is media sanitized for reuse? *FISCAM AC-3.4* *NIST SP 800-18*								
8.2.9 Is damaged media stored and /or destroyed? *NIST SP 800-18*								
8.2.10 Is hardcopy media shredded or destroyed when no longer needed? *NIST SP 800-18*								

NOTES:

9. Contingency Planning

Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Contingency Planning *OMB Circular A-130, III*								
9.1. Critical Element: **Have the most critical and sensitive operations and their supporting computer resources been identified?**								
9.1.1 Are critical data files and operations identified and the frequency of file backup documented? *FISCAM SC- SC-1.1 & 3.1* *NIST SP 800-18*								
9.1.2 Are resources supporting critical operations identified? *FISCAM SC-1.2*								
9.1.3 Have processing priorities been established and approved by management? *FISCAM SC-1.3*								
9.2. Critical Element: **Has a comprehensive contingency plan been developed and documented?**								
9.2.1 Is the plan approved by key affected parties? *FISCAM SC-3.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
9.2.2 Are responsibilities for recovery assigned? *FISCAM SC-3.1*								
9.2.3 Are there detailed instructions for restoring operations? *FISCAM SC-3.1*								
9.2.4 Is there an alternate processing site; if so, is there a contract or interagency agreement in place? *FISCAM SC-3.1* *NIST SP 800-18*								
9.2.5 Is the location of stored backups identified? *NIST SP 800-18*								
9.2.6 Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged? *FISCAM SC-2.1*								
9.2.7 Is system and application documentation maintained at the off-site location? *FISCAM SC-2.1*								
9.2.8 Are all system defaults reset after being restored from a backup? *FISCAM SC-3.1*								
9.2.9 Are the backup storage site and alternate site geographically removed from the primary site and physically protected? *FISCAM SC-2.1*								
9.2.10 Has the contingency plan been distributed to all appropriate personnel? *FISCAM SC-3.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
9.3. Critical Element: Are tested contingency/disaster recovery plans in place?								
9.3.1 Is an up-to-date copy of the plan stored securely off-site? *FISCAM SC-3.1*								
9.3.2 Are employees trained in their roles and responsibilities? *FISCAM SC-2.3 NIST SP 800-18*								
9.3.3 Is the plan periodically tested and readjusted as appropriate? *FISCAM SC-3.1 NIST SP 800-18*								

NOTES:

10. Hardware and System Software Maintenance

These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. Some of these controls are also covered in the Life Cycle Section. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Hardware and System Software Maintenance *OMB Circular A-130, III*								
10.1. Critical Element: **Is access limited to system software and hardware?**								
10.1.1 Are restrictions in place on who performs maintenance and repair activities? *OMB Circular A-130, III* *FISCAM SS-3.1* *NIST SP 800-18*								
10.1.2 Is access to all program libraries restricted and controlled? *FISCAM CC-3.2 & 3.3*								
10.1.3 Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls? *FISCAM SS-1.2*								
10.1.5 Are up-to-date procedures in place for using and monitoring use of system utilities? *FISCAM SS-2.1*								
10.2. Critical Element: Are all new and revised hardware and software authorized, tested and approved before implementation?								
10.2.1 Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control? *NIST SP 800-18*								
10.2.2 Are system components tested, documented, and approved (operating system, utility, applications) prior to promotion to production? *FISCAM SS-3.1, 3.2, & CC-2.1* *NIST SP 800-18*								
10.2.3 Are software change request forms used to document requests and related approvals? *FISCAM CC-1.2* *NIST SP 800-18*								
10.2..4 Are there detailed system specifications prepared and reviewed by management? *FISCAM CC-2.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.5 Is the type of test data to be used specified, i.e., live or made up? *NIST SP 800-18*								
10.2.6 Are default settings of security features set to the most restrictive mode? *PSN Security Assessment Guidelines*								
10.2.7 Are there software distribution implementation orders including effective date provided to all locations? *FISCAM CC-2.3*								
10.2.8 Is there version control? *NIST SP 800-18*								
10.2.9 Are programs labeled and inventoried? *FISCAM CC-3.1*								
10.2.10 Are the distribution and implementation of new or revised software documented and reviewed? *FISCAM SS-3.2*								
10.2.11 Are emergency change procedures documented and approved by management, either prior to the change or after the fact? *FISCAM CC-2.2*								
10.2.12 Are contingency plans and other associated documentation updated to reflect system changes? *FISCAM SC-2.1* *NIST SP 800-18*								
10.2.13 Is the use of copyrighted software or shareware and personally owned software/equipment documented? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.3. Are systems managed to reduce vulnerabilities?								
10.3.1 Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls)? *NIST SP 800-18*								
10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed? *NIST SP 800-18*								

NOTES:

11. Data Integrity

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user the information meets expectations about its quality and integrity. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Data Integrity *OMB Circular A-130, 8B3*								
11.1. Critical Element: Is virus detection and elimination software installed and activated?								
11.1.1 Are virus signature files routinely updated? *NIST SP 800-18*								
11.1.2 Are virus scans automatic? *NIST SP 800-18*								
11.2. Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?								
11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
11.2.2 Is inappropriate or unusual activity reported, investigated, and appropriate actions taken? *FISCAM SS-2.2*								
11.2.3 Are procedures in place to determine compliance with password policies? *NIST SP 800-18*								
11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? *NIST SP 800-18*								
11.2.5 Are intrusion detection tools installed on the system? *NIST SP 800-18*								
11.2.6 Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly? *NIST SP 800-18*								
11.2.7 Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks? *NIST SP 800-18*								
11.2.8 Is penetration testing performed on the system? *NIST SP 800-18*								
11.2.9 Is message authentication used? *NIST SP 800-18*								

NOTES:

12. Documentation

The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system document and formalize the system's security controls. When answering whether there are procedures for each control objective, the question should be phrased "are there procedures for ensuring the documentation is obtained and maintained." The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Documentation *OMB Circular A-130, 8B3*								
12.1. Critical Element: **Is there sufficient documentation that explains how software/hardware is to be used?**								
12.1.1 Is there vendor-supplied documentation of purchased software? *NIST SP 800-18*								
12.1.2 Is there vendor-supplied documentation of purchased hardware? *NIST SP 800-18*								
12.1.3 Is there application documentation for in-house applications? *NIST SP 800-18*								
12.1.4 Are there network diagrams and documentation on setups of routers and switches? *NIST SP 800-18*								
12.1.5 Are there software and hardware testing procedures and results? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
12.1.6 Are there standard operating procedures for all the topic areas covered in this document? *NIST SP 800-18*								
12.1.7 Are there user manuals? *NIST SP 800-18*								
12.1.8 Are there emergency procedures? *NIST SP 800-18*								
12.1.9 Are there backup procedures? *NIST SP 800-18*								
12.2. Critical Element: **Are there formal security and operational procedures documented?**								
12.2.1 Is there a system security plan? *OMB Circular A-130, III* *FISCAM SP-2.1* *NIST SP 800-18*								
12.2.2 Is there a contingency plan? *NIST SP 800-18*								
12.2.3 Are there written agreements regarding how data is shared between interconnected systems? *OMB A-130, III* *NIST SP 800-18*								
12.2.4 Are there risk assessment reports? *NIST SP 800-18*								
12.2.5 Are there certification and accreditation documents and a statement authorizing the system to process? *NIST SP 800-18*								

NOTES:

13. Security Awareness, Training, and Education

People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Security Awareness, Training, and Education *OMB Circular A-130, III*								
13.1. Critical Element: Have employees received adequate training to fulfill their security responsibilities?								
13.1.1 Have employees received a copy of the Rules of Behavior? *NIST SP 800-18*								
13.1.2 Are employee training and professional development documented and monitored? *FISCAM SP-4.2*								
13.1.3 Is there mandatory annual refresher training? *OMB Circular A-130, III*								
13.1.4 Are methods employed to make employees aware of security, i.e., posters, booklets? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
13.1.5 Have employees received a copy of or have easy access to agency security procedures and policies? *NIST SP 800-18*								

NOTES:

14. Incident Response Capability

Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and their impact far-reaching. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Incident Response Capability *OMB Circular A-130, III* *FISCAM SP-3.4* *NIST 800-18*								
14.1. Critical Element: **Is there a capability to provide help to users when a security incident occurs in the system?**								
14.1.1 Is a formal incident response capability available? *FISCAM SP-3.4* *NIST SP 800-18*								
14.1.2 Is there a process for reporting incidents? *FISCAM SP-3.4* *NIST SP 800-18*								
14.1.3 Are incidents monitored and tracked until resolved? *NIST SP 800-18*								
14.1.4 Are personnel trained to recognize and handle incidents? *FISCAM SP-3.4* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
14.1.5 Are alerts/advisories received and responded to? *NIST SP 800-18*								
14.1.6 Is there a process to modify incident handling procedures and control techniques after an incident occurs? *NIST SP 800-18*								
14.2. Critical Element: **Is incident related information shared with appropriate organizations?**								
14.2.1 Is incident information and common vulnerabilities or threats shared with owners of interconnected systems? *OMB A-130, III* *NIST SP 800-18*								
14.2.2 Is incident information shared with FedCIRC[3] concerning incidents and common vulnerabilities and threats? *OMB A-130, III* *GISRA*								
14.2.3 Is incident information reported to FedCIRC, NIPC[4], and local law enforcement when necessary? *OMB A-130,III* *GISRA*								

[3] FedCIRC (Federal Computer Incident Response Capability) is the U.S. Government's focal point for handling computer security-related incidents.

[4] NIPC's mission is to serve as the U.S. Government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures.

NOTES:

Technical Controls

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

15. Identification and Authentication

Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Identification and Authentication *OMB Circular A-130, III* *FISCAM AC-2* *NIST SP 800-18*								
15.1. Critical Element: **Are users individually authenticated via passwords, tokens, or other devices?**								
15.1.1 Is a current list maintained and approved of authorized users and their access? *FISCAM AC-2* *NIST SP 800-18*								
15.1.2 Are digital signatures used and conform to FIPS 186-2? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.3 Are access scripts with embedded passwords prohibited? *NIST SP 800-18*								
15.1.4 Is emergency and temporary access authorized? *FISCAM AC-2.2*								
15.1.5 Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access? *FISCAM AC-3.2*								
15.1.6 Are passwords changed at least every ninety days or earlier if needed? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.8 Are inactive user identifications disabled after a specified period of time? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.9 Are passwords not displayed when entered? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.10 Are there procedures in place for handling lost and compromised passwords? *FISCAM AC-3.2* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.11 Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)? *NIST SP 800-18*								
15.1.12 Are passwords transmitted and stored using secure protocols/algorithms? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.13 Are vendor-supplied passwords replaced immediately? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.14 Is there a limit to the number of invalid access attempts that may occur for a given user? *FISCAM AC-3.2* *NIST SP 800-18*								
15.2. Critical Element: Are access controls enforcing segregation of duties?								
15.2.1 Does the system correlate actions to users? *OMB A-130, III* *FISCAM SD-2.1*								
15.2.2 Do data owners periodically review access authorizations to determine whether they remain appropriate? *FISCAM AC-2.1*								

NOTES:

16. Logical Access Controls

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Logical Access Controls *OMB Circular A-130, III* *FISCAM AC-3.2* *NIST SP 800-18*								
16.1. Critical Element: **Do the logical access controls restrict users to authorized transactions and functions?**								
16.1.1 Can the security controls detect unauthorized access attempts? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.2 Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.3 Is access to security software restricted to security administrators? *FISCAM AC-3.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.1.4 Do workstations disconnect or screen savers lock system after a specific period of inactivity? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.5 Are inactive users' accounts monitored and removed when not needed? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.6 Are internal security labels (naming conventions) used to control access to specific information types or files? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.7 If encryption is used, does it meet federal standards? *NIST SP 800-18*								
16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? *NIST SP 800-18*								
16.1.9 Is access restricted to files at the logical view or field? *FISCAM AC-3.2*								
16.1.10 Is access monitored to identify apparent security violations and are such events investigated? *FISCAM AC-4*								
16.2. Critical Element: **Are there logical controls over network access?**								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.1 Has communication software been implemented to restrict access through specific terminals? *FISCAM AC-3.2*								
16.2.2 Are insecure protocols (e.g., UDP, ftp) disabled? *PSN Security Assessment Guidelines*								
16.2.3 Have all vendor-supplied default security parameters been reinitialized to more secure settings? *PSN Security Assessment Guidelines*								
16.2.4 Are there controls that restrict remote access to the system? *NIST SP 800-18*								
16.2.5 Are network activity logs maintained and reviewed? *FISCAM AC-3.2*								
16.2.6 Does the network connection automatically disconnect at the end of a session? *FISCAM AC-3.2*								
16.2.7 Are trust relationships among hosts and external entities appropriately restricted? *PSN Security Assessment Guidelines*								
16.2.8 Is dial-in access monitored? *FISCAM AC-3.2*								
16.2.9 Is access to telecommunications hardware or facilities restricted and monitored? *FISCAM AC-3.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.10 Are firewalls or secure gateways installed? *NIST SP 800-18*								
16.2.11 If firewalls are installed do they comply with firewall policy and rules? *FISCAM AC-3.2*								
16.2.12 Are guest and anonymous accounts authorized and monitored? *PSN Security Assessment Guidelines*								
16.2.13 Is an approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished? *FISCAM AC-3.2* *NIST SP 800-18*								
16.2.14 Are sensitive data transmissions encrypted? *FISCAM AC-3.2*								
16.2.15 Is access to tables defining network options, resources, and operator profiles restricted? *FISCAM AC-3.2*								
16.3. Critical Element: **If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?**								
16.3.1 Is a privacy policy posted on the web site? *OMB-99-18*								

NOTES:

17. Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. The following questions are organized under one critical element. The levels for the critical element should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Audit Trails *OMB Circular A-130, III* *FISCAM AC-4.1* *NIST SP 800-18*								
17.1. Critical Element: **Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?**								
17.1.1 Does the audit trail provide a trace of user actions? *NIST SP 800-18*								
17.1.2 Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased? *NIST SP 800-18*								
17.1.3 Is access to online audit logs strictly controlled? *NIST SP 800-18*								
17.1.4 Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
17.1.5 Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail? *NIST SP 800-18*								
17.1.6 Are audit trails reviewed frequently? *NIST SP 800-18*								
17.1.7 Are automated tools used to review audit records in real time or near real time? *NIST SP 800-18*								
17.1.8 Is suspicious activity investigated and appropriate action taken? *FISCAM AC-4.3*								
17.1.9 Is keystroke monitoring used? If so, are users notified? *NIST SP 800-18*								

NOTES:

Appendix B – Source of Control Criteria

Office of Management and Budget Circular A-130, "Management of Federal Information Resources", Section 8B3 and Appendix III, "Security of Federal Automated Information Resources."	Establishes a minimum set of controls to be included in Federal IT security programs.
Computer Security Act of 1987.	This statute set the stage for protecting systems by codifying the requirement for Government-wide IT security planning and training.
Paperwork Reduction Act of 1995.	The PRA established a comprehensive information resources management framework including security and subsumed the security responsibilities of the Computer Security Act of 1987.
Clinger-Cohen Act of 1996.	This Act linked security to agency capital planning and budget processes, established agency Chief Information Officers, and re-codified the Computer Security Act of 1987.
Presidential Decision Directive 63, "Protecting America's Critical Infrastructures."	This directive specifies agency responsibilities for protecting the nation's infrastructure, assessing vulnerabilities of public and private sectors, and eliminating vulnerabilities.
OMB Memorandum 99-18, "Privacy Policies on Federal Web Sites."	This memorandum directs Departments and Agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing so.
General Accounting Office "Federal Information System Control Audit Manual" (FISCAM).	The FISCAM methodology provides guidance to auditors in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.
NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Security Information Technology Systems."	This publication guides organizations on the types of controls, objectives, and procedures that comprise an effective security program.
NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems."	This publication details the specific controls that should be documented in a system security plan.
Defense Authorization Act (P.L. 106-398) including Title X, Subtitle G, "Government Information Security Reform" (GISRA)	The act primarily addresses the program management and evaluation aspects of security.
Office of the Manager, National Communications Systems, "Public Switched Network Security Assessment Guidelines."	The guide describes a risk assessment procedure, descriptions of a comprehensive security program, and a summary checklist.
Federal Information Processing Standards.	These documents contain mandates and/or guidance for improving the utilization and management of computers and IT systems in the Federal Government.

Federal Information Technology Security Assessment Framework

November 28, 2000

Prepared for

Security, Privacy, and Critical Infrastructure Committee

by

National Institute of Standards and Technology (NIST)
Computer Security Division

Overview

Information and the systems that process it are among the most valuable assets of any organization. Adequate security of these assets is a fundamental management responsibility. Consistent with Office of Management and Budget (OMB) policy, each agency must implement and maintain a program to adequately secure its information and system assets. Agency 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, and ensure that the appropriate officials are assigned security responsibility 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 security programs and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

The Federal Information Technology (IT) Security Assessment Framework (or Framework) provides a method for agency officials to 1) determine the current status of their security programs relative to existing policy and 2) where necessary, establish a target for improvement. It does not establish new security requirements. The Framework may be used to assess the status of security controls for a given asset or collection of assets. These assets include information, individual systems (e.g., major applications, general support systems, mission critical systems), or a logically related grouping of systems that support operational programs, or operational programs (e.g., Air Traffic Control, Medicare, Student Aid). Assessing all asset security controls and all interconnected systems that the asset depends on produces a picture of both the security condition of an agency component and of the entire agency.

The Framework comprises five levels to guide agency assessment of their security programs and assist in prioritizing efforts for improvement. Coupled with the NIST-prepared self-assessment questionnaire[5], the Framework provides a vehicle for consistent and effective measurement of the security status for a given asset. The security status is measured by determining if specific security controls are documented, implemented, tested and reviewed, and incorporated into a cyclical review/improvement program, as well as whether unacceptable risks are identified and mitigated. The NIST questionnaire provides specific questions that identify the control criteria against which agency policies, procedures, and security controls can be compared. Appendix A contains a sample of the upcoming NIST Special Publication.

The Framework is divided into five levels: Level 1 of the Framework reflects that an asset has documented security policy. At level 2, the asset also has documented procedures and controls to implement the policy. Level 3 indicates that procedures and

[5] The NIST Self-assessment Questionnaire will be issued in 2001 as a NIST Special Publication.

controls have been implemented. Level 4 shows that the procedures and controls are tested and reviewed. At level 5, the asset has procedures and controls fully integrated into a comprehensive program. Each level represents a more complete and effective security program. OMB and the Council recognize that the security needs for the tens of thousands of Federal information systems differ. Agencies should note that testing the effectiveness of the asset and all interconnected systems that the asset depends on is essential to understanding whether risk has been properly mitigated. When an individual system does not achieve level 4, agencies should determine whether that system meets the criteria found in OMB Memorandum M00-07 (February 28, 2000) "Incorporating and Funding Security in Information Systems Investments." Agencies should seek to bring all assets to level 4 and ultimately level 5.

Integral to all security programs whether for an asset or an entire agency is a risk assessment process that includes determining the level of sensitivity of information and systems. Many agencies have developed their own methods of making these determinations. For example, the Department of Health and Human Services uses a four--track scale for confidentiality, integrity, and availability. The Department of Energy uses five groupings or "clusters" to address sensitivity. Regardless of the method used, the asset owner is responsible for determining how sensitive the asset is, what level of risk is acceptable, and which specific controls are necessary to provide adequate security to that asset. Again, each implemented security control must be periodically tested for effectiveness. The decision to implement and the results of the testing should be documented.

1. Framework Description

The Federal Information Technology Security Assessment Framework (Framework) identifies five levels of IT security program effectiveness (see Figure 1). The five levels measure specific management, operational, and technical control objectives. Each of the five levels contains criteria to determine if the level is adequately implemented. For example, in Level 1, all written policy should contain the purpose and scope of the policy, the individual(s) responsible for implementing the policy, and the consequences and penalties for not following the policy. The policy for an individual control must be reviewed to ascertain that the criteria for level 1 are met. Assessing the effectiveness of the individual controls, not simply their existence, is key to achieving and maintaining adequate security.

The asset owner, in partnership with those responsible for administering the information assets (which include IT systems), must determine whether the measurement criteria are being met at each level. Before making such a determination, the degree of sensitivity of information and systems must be determined by considering the requirements for confidentiality, integrity, and availability of both the information and systems -- the value of information and systems is one of the major factors in risk management.

A security program may be assessed at various levels within an organization. For example, a program could be defined as an agency asset, a major application, general support system, high impact program, physical plant, mission critical system, or logically related group of systems. The Framework refers to this grouping as an asset.

The Framework describes an asset self-assessment and provides levels to guide and prioritize agency efforts as well as a basis to measure progress. In addition, the National Institute of Standards and Technology (NIST) will develop a questionnaire that gives the implementation tools for the Framework. The questionnaire will contain specific control objectives that should be applied to secure a system.

Figure 1 – Federal IT Security Assessment Framework

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

The Framework approach begins with the premise that all agency assets must meet the minimum security requirements of the Office of Management and Budget Circular A-130, “Management of Federal Resources”, Appendix III, “Security of Federal Automated Information Resources” (A-130). The criteria that are outlined in the Framework and provided in detail in the questionnaire are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy. It should be noted that an agency might have additional laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability. Each agency should decide if additional security controls should be added to the questionnaire and, if so, customize the questionnaire appropriately. A list of the documents that the Framework and the questionnaire draw upon is provided in Figure 2.

Figure 2 – Source of Control Criteria

Office of Management and Budget Circular A-130, "Management of Federal Information Resources", Appendix III, "Security of Federal Automated Information Resources."	Establishes a minimum set of controls to be included in Federal IT security programs.
Computer Security Act of 1987.	This statute set the stage for protecting systems by codifying the requirement for Government-wide IT security planning and training.
Paperwork Reduction Act of 1995.	The PRA established a comprehensive information resources management framework including security and subsumed the security responsibilities of the Computer Security Act of 1987.
Clinger-Cohen Act of 1996.	This Act linked security to agency capital planning and budget processes, established agency Chief Information Officers, and re-codified the Computer Security Act of 1987.
Presidential Decision Directive 63, "Protecting America's Critical Infrastructures."	This directive specifies agency responsibilities for protecting the nation's infrastructure, assessing vulnerabilities of public and private sectors, and eliminating vulnerabilities.
Presidential Decision Directive 67, "Enduring Constitutional Government and Continuity of Government."	Relates to ensuring constitutional government, continuity of operations (COOP) planning, and continuity of government (COG) operations
OMB Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records."	This memorandum provides instructions to agencies on how to comply with the President's Memorandum of May 14, 1998 on "Privacy and Personal Information in Federal Records."
OMB Memorandum 99-18, "Privacy Policies on Federal Web Sites."	This memorandum directs Departments and Agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing so.
OMB Memorandum 00-13, "Privacy Policies and Data Collection on Federal Web Sites."	The purpose of this memorandum is a reminder that each agency is required by law and policy to establish clear privacy policies for its web activities and to comply with those policies.
General Accounting Office "Federal Information System Control Audit Manual" (FISCAM).	The FISCAM methodology provides guidance to auditors in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.
NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Security Information Technology Systems."	This publication guides organizations on the types of controls, objectives, and procedures that comprise an effective security program.
NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems."	This publication details the specific controls that should be documented in a system security plan.
Federal Information Processing Standards.	This document contains legislative and executive mandates for improving the utilization and management of computers and IT systems in the Federal Government.

2. Documented Policy - Level 1

2.1 Description

Level 1 of the Framework includes:

- Formally documented and disseminated security policy covering agency headquarters and major components (e.g., bureaus and operating divisions). The policy may be asset specific.
- Policy that references most of the basic requirements and guidance issued from the documents listed in Figure 2 – Source of Control Criteria.

An asset is at level 1 if there is a formally, up-to-date 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. The criteria listed below should be applied when assessing the policy developed for the controls that are listed in the NIST questionnaire.

2.2 Criteria

Level 1 criteria describe the components of a security policy.

Criteria for Level 1
a. Purpose and scope. An up-to-date security policy is written that covers all major facilities and operations agency-wide or for the asset. The policy is approved by key affected parties and covers security planning, risk management, review of security controls, rules of behavior, life-cycle management, processing authorization, personnel, physical and environmental aspects, computer support and operations, contingency planning, documentation, training, incident response, access controls, and audit trails. The policy clearly identifies the purpose of the program and its scope within the organization.
b. Responsibilities. The security program comprises a security management structure with adequate authority, and expertise. IT security manager(s) are appointed at an overall level and at appropriate subordinate levels. Security responsibilities and expected behaviors are clearly defined for asset owners and users, information resources management and data processing personnel, senior management, and security administrators.
c. Compliance. General compliance and specified penalties and disciplinary actions are also identified in the policy.

3. Documented Procedures - Level 2

3.1 Description

Level 2 of the Framework includes:

- Formal, complete, well-documented procedures for implementing policies established at level one.
- The basic requirements and guidance issued from the documents listed in Figure 2 – Source of Control Criteria.

An asset 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 assets.

Well-documented and current security procedures are necessary to ensure that adequate and cost effective security controls are implemented. The criteria listed below should be applied when assessing the quality of the procedures for controls outlined in the NIST questionnaire.

3.2 Criteria

Level 2 criteria describe the components of security procedures.

Criteria for Level 2
a. Control areas listed and organization's position stated. Up-to-date procedures are written that covers all major facilities and operations within the asset. The procedures are approved by key responsible parties and cover security policies, security plans, risk management, review of security controls, rules of behavior, life-cycle management, processing authorization, personnel, physical and environmental aspects, computer support and operations, contingency planning, documentation, training, incident response, access controls, and audit trails. The procedures clearly identify management's position and whether there are further guidelines or exceptions.
b. Applicability of procedures documented. Procedures clarify where, how, when, to, whom, and about what a particular procedure applies.
c. Assignment of IT security responsibilities and expected behavior. Procedures clearly define security responsibilities and expected behaviors for (1) asset owners and users, (2) information resources management and data processing personnel, (3) management, and (4) security administrators.
d. Points of contact and supplementary information provided. Procedures contain appropriate individuals to be contacted for further information, guidance, and compliance.

4. Implemented Procedures and Controls - Level 3

4.1 Description

Level 3 of the Framework includes:

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

At level 3, the IT security procedures and controls are implemented in a consistent manner and reinforced through training. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. Security controls for an asset 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 on-going effectiveness is not emphasized in level 3, some testing is needed when initially implementing controls to ensure they are operating as intended. The criteria listed below should be used to determine if the specific controls listed in the NIST questionnaire are being implemented.

4.2 Criteria

Level 3 criteria describe how an organization can ensure implementation of their security procedures.

Criteria for Level 3
a. Owners and users are made aware of security policies and procedures. Security policies and procedures are distributed to all affected personnel, including system/application rules and expected behaviors. Requires users to periodically acknowledge their awareness and acceptance of responsibility for security.
b. Policies and procedures are formally adopted and technical controls installed. Automated and other tools routinely monitor security. Established policy governs review of system logs, penetration testing, and internal/external audits.
c. Security is managed throughout the life cycle of the system. Security is considered in each of the life-cycle phases: initiation, development/acquisition, implementation, operation, and disposal.
d. Procedures established for authorizing processing (certification and accreditation). Management officials must formally authorize system operations and manage risk.
e. Documented security position descriptions. Skill needs and security responsibilities in job descriptions are accurately identified.
f. Employees trained on security procedures. An effective training and awareness program tailored for varying job functions is planned, implemented, maintained, and evaluated.

5. Tested and Evaluated Procedures and Controls - Level 4

5.1 Description

Level 4 of the Framework 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 FedCIRC, vendors, and other trusted sources.

Routine evaluations 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, data sensitivity) and ensuring that security policies and procedures are appropriate and are operating as intended on an ongoing basis.

Routine self-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. Self-assessments can be performed by agency staff or by contractors or others engaged by agency management. Independent audits such as those arranged by the General Accounting Office (GAO) or an agency Inspector General (IG), are an important check on agency performance, but should not be viewed as a substitute for evaluations initiated by agency management.

To be effective, routine evaluations must include tests and examinations of key controls. Reviews of documentation, walk-throughs 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, evaluations must include security controls of interconnected assets, e.g., network supporting applications being tested.

When assets are first implemented or are modified, they should be tested and certified to ensure that 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 evaluation program.

In addition to test results, agency evaluations 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.

The criteria listed below should be applied to each control area listed in the NIST questionnaire to determine if the asset is being effectively evaluated.

5.2 Criteria

Level 4 criteria are listed below.

Criteria for Level 4
a. Effective program for evaluating adequacy and effectiveness of security policies, procedures, and controls. Evaluation requirements, including requirements regarding the type and frequency of testing, should be documented, approved, and effectively implemented. The frequency and rigor with which individual controls are tested should depend on the risks that will be posed if the controls are not operating effectively. At a minimum, controls should be evaluated whenever significant system changes are made or when other risk factors, such as the sensitivity of data processed, change. Even controls for inherently low-risk operations should be tested at a minimum of every 3 years.
b. Mechanisms for identifying vulnerabilities revealed by security incidents or security alerts. Agencies should routinely analyze security incident records, including any records of anomalous or suspicious activity that may reveal security vulnerabilities. In addition, they should review security alerts issued by FedCIRC, vendors, and others.
c. Process for reporting significant security weaknesses and ensuring effective remedial action. *Such a process should provide for routine reports to senior management on weaknesses identified through testing or other means, development of action plans, allocation of needed resources, and follow-up reviews to ensure that remedial actions have been effective. Expedited processes should be implemented for especially significant weaknesses that may present undue risk if not addressed immediately.*

6. Fully Integrated Procedures and Controls - Level 5

6.1 Description

Level 5 of the Framework 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 IT security is pervasive in the culture of a level 5 asset. 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 IT life cycle include:

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

Each of these decisions result 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. Entities should apply the principle of selecting controls that offer the lowest cost implementation while offering adequate risk mitigation, versus high cost implementation and low risk mitigation. The criteria listed below should be used to assess whether a specific control contained in the NIST questionnaire has been fully implemented.

6.2 Criteria

Level 5 criteria describe components of a fully integrated security program.

Criteria for Level 5
a. There is an active enterprise-wide security program that achieves cost-effective security.
b. IT security is an integrated practice within the asset.
c. Security vulnerabilities are understood and managed.
d. Threats are continually re-evaluated, and controls adapted to changing security environment.
e. Additional or more cost-effective security alternatives are identified as the need arises.
f. Costs and benefits of security are measured as precisely as practicable.
g. Status metrics for the security program are established and met.

7. Future of the Framework

This version of the Framework primarily addresses security management issues. It describes a process for agencies to assess their compliance with long-standing basic requirements and guidance. With the Framework in place, agencies will have an approach to begin the assessment process. The NIST questionnaire provides the tool to determine whether agencies are meeting these requirements and following the guidance.

The Framework is not static; it is a living document. Revisions will focus on expanding, refining, and providing more granularity for existing criteria. In addition, the establishment of a similar companion framework devoted to the evolution of agency electronic privacy polices may be considered in time.

The Framework can be viewed as both an auditing tool and a management tool. A balance between operational needs and cost effective security for acceptable risk will need to be made to achieve an adequate level of security.

Currently, the NIST self-assessment tool is under development and will be available in 2001. Appendix A provides a sample questionnaire to assist agencies until NIST officially releases the questionnaire.

Appendix A
Conceptual Sample of NIST Self-Assessment Questionnaire

Below is a conceptual sample of the Hypothetical Government Agency's (HGA) completion of the NIST questionnaire for their Training Database. Before the questionnaire was completed, the sensitivity of the information stored within, processed by and transmitted by this asset was assessed. The premise behind determining the level of sensitivity is that each asset owner is responsible for determining what level of risk is acceptable, and which specific security controls are necessary to provide adequate security.

The sensitivity of this asset was determined to be high for confidentiality and low for integrity and availability. The confidentiality of the system is high due to the system containing personnel information. Employee social security numbers, course lists, and grades are contained in the system. The integrity of the database is considered low because if the information were modified by unauthorized, unanticipated or unintentional means, employees, who can read their own training file, would detect the modifications. The availability of the system is considered low because hard copies of the training forms are available as a backup.

The questionnaire was completed for the database with the understanding that security controls that protect the integrity or availability of the data did not have to be rigidly applied. The questionnaire contains a field that can be checked when a risk-based decision has been made to either reduce or enhance a security control. There may be certain situations where management will grant a waiver either because compensating controls exist or because the benefits of operating without the control (at least temporarily) outweigh the risk of waiting for full control implementation. Alternatively, there may be times where management implements more stringent controls than generally applied elsewhere. In the example provided the specific control objectives for personnel security and for authentication were assessed. The questionnaire is an excerpt and by no means contains all the questions that would be asked in the area of personnel security and authentication. For brevity, only a few questions were provided in this sample.

An analysis of the levels checked determined that the agency should target improving their background screening implementation and testing. System administrators, programmers, and managers should all have background checks completed prior to accessing the system. The decision to allow access prior to screening was made and checked in the *Risk Based Decision Made* box. Because this box was checked, there should be specific controls implemented to ensure access is not abused, i.e., access is reviewed daily through audit trails, and users have minimal system authority.

Additionally, HGA should improve implementing and testing their password procedures because of the strong need for confidentiality. Without good password management, passwords can be easily guessed and access to the system obtained. The questionnaire's list of objectives is incomplete for both personnel security controls and for authentication controls. Even though the sample is lacking many controls, the completed questionnaire

clearly depicts that HGA has policies and procedures in place but there is a strong need for implementing, testing, and reviewing the procedures and controls. The sample indicates that the Training Database would be at level 2.

Category of Sensitivity	Confidentiality	Integrity	Availability
High	X		
Medium			
Low		X	X

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made
Personnel Security						
Are all positions reviewed for sensitivity level?	X	X	X			
Is appropriate background screening for assigned positions completed prior to granting access?	X	X				X
Are there conditions for allowing system access prior to completion of screening?	X	X				
Are sensitive functions divided among different individuals?	X	X	X			
Are mechanisms in place for holding users responsible for their actions?	X	X				
Are termination procedures established?	X	X				
Authentication						
Are passwords, tokens, or biometrics used?	X	X	X			
Do passwords contain alpha numeric, upper/lower case, and special characters?	X	X				
Are passwords changed at least every ninety days or earlier if needed?	X	X				
Is there guidance for handling lost and compromised passwords?	X	X				
Are passwords transmitted and stored with one-way encryption?	X	X				
Is there a limit to the number of invalid access attempts that may occur for a given user?	X	X				

References

Automated Information Systems Security Program Handbook (Release 2.0, May 1994), Department of Health and Human Services, May 1994.

Clinger-Cohen Act of 1996 (formerly known as the Information Management Reform Act), February 10, 1996.

Computer Security Act of 1987, 40 U.S. Code 759, (Public Law 100-235), January 8, 1988.

Control Objectives for Information and Related Technology (COBIT) 3rd Edition, Information Systems Audit and Control Foundation, July 2000.

General Accounting Office, Federal Information System Control Audit Manual (FISCAM), GOA/AIMD-12.19.6, January 1999.

General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, GAO/AIMD-99-139, August 1999.

Office of Management and Budget, Security of Federal Automated Information Resources, Appendix III to OMB Circular A-130, Management of Federal Information Resources, February 8, 1996.

Office of Management and Budget, Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, Privacy and Personal Information in Federal Records, July 1, 1999.

Office of Management and Budget, Memorandum 99-18, Privacy Policies on Federal Web Sites, June 2, 1999.

Office of Management and Budget, Memorandum 00-13, Policies and Data Collection on Federal Web Sites, June 22, 2000.

Paperwork Reduction Act of 1995, 35 U.S. Code 44, January 4, 1995.

Presidential Decision Directive 63, Protecting America's Critical Infrastructures, May 22, 1998.

Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government, October 21, 1998.

Swanson, Marianne and Barbara Guttman, NIST Special Publication 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP), Gaithersburg, MD, National Institute of Standards and Technology, September 20, 1995.

Swanson, Marianne and Federal Computer Security Program Managers' Forum Working Group, NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, Gaithersburg, MD, National Institute of Standards and Technology, December 1998.

Terminology

Acceptable Risk is a concern that is acceptable to responsible management, due to the cost and magnitude of implementing controls.

Accreditation is synonymous with the term **authorize processing**. Accreditation is the authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security. See also ***Authorize Processing, Certification,*** and ***Designated Approving Authority.***

Asset is a major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems.

Authorize Processing occurs when management authorizes in writing a system based on an assessment of management, operational, and technical controls. By authorizing processing in a system the management official accepts the risks associated with it. See also ***Accreditation, Certification,*** and ***Designated Approving Authority.***

Availability Protection requires backup of system and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical applications, time and attendance, financial, procurement, or life-critical.

Awareness, Training, and Education includes (1) awareness programs set the stage for training by changing organizational attitudes towards 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 IT security.

Certification is synonymous with the term **authorize processing.** Certification is a major consideration prior to authorizing processing, but not the only consideration. Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meets a pre-specified set of security requirements. See also ***Accreditation*** and ***Authorize Processing.***

General Support System is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Individual Accountability requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

Information Owner is responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that responsibility even when the data/information are shared with other organizations.

Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Material Weakness or ***significant weakness*** is used to identify control weaknesses that pose a significant risk or a threat to the operations and/or assets of an audited entity. "Material weakness" is a very specific term that is defined one way for financial audits and another way for weaknesses reported under the Federal Managers Financial Integrity Act of 1982. Such weaknesses may be identified by auditors or by management.

Networks include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet.

Operational Controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

Policy a document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.

Procedures are contained in a document that focuses on the security control areas and management's position.

Risk is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Management is the ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Rules of Behavior are 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, assignment and limitation of system privileges, and individual accountability.

Sensitive Information refers to information whose loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled.

Sensitivity an information technology environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and/or availability that is determined by an evaluation of the sensitivity of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.

System is a generic term used for briefness to mean either a major application or a general support system.

System Operational Status is either (1) Operational - system is currently in operation, (2) Under Development - system is currently under design, development, or implementation, or (3) Undergoing a Major Modification - system is currently undergoing a major conversion or transition.

Technical Controls consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Threat is an event or activity, deliberate or unintentional, with the potential for causing harm to an IT system or activity.

Vulnerability is a flaw or weakness that may allow harm to occur to an IT system or activity.

Appendix D - References

Clinger-Cohen Act of 1996 (formerly known as the Information Management Reform Act), February 10, 1996.

Computer Security Act of 1987, 40 U.S. Code 759, (Public Law 100-235), January 8, 1988.

Control Objectives for Information and Related Technology (COBIT) 3rd Edition, Information Systems Audit and Control Foundation, July 2000.

Defense Authorization Act (P.L. 106-398) including Title X, Subtitle G, "Government Information Security Reform," October 28, 2000.

Department of State, Draft Best Security Practices Checklist Appendix A, January 22, 2001.

General Accounting Office, Federal Information System Control Audit Manual (FISCAM), GOA/AIMD-12.19.6, January 1999.

General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, GAO/AIMD-99-139, August 1999.

ISSO 17799, A Code of Practice for Information Security Management (British Standard 7799),

National Communications System, Public Switched Network Security Assessment Guidelines, September 2000.

Office of Management and Budget, Security of Federal Automated Information Resources, Appendix III to OMB Circular A-130, Management of Federal Information Resources, February 8, 1996.

Office of Management and Budget, Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, Privacy and Personal Information in Federal Records, July 1, 1999.

Office of Management and Budget, Memorandum 99-18, Privacy Policies on Federal Web Sites, June 2, 1999.

Office of Management and Budget, Memorandum 00-13, Policies and Data Collection on Federal Web Sites, June 22, 2000.

Paperwork Reduction Act of 1995, 35 U.S. Code 44, January 4, 1995.

Presidential Decision Directive 63, Protecting America's Critical Infrastructures, May 22, 1998.

Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government, October 21, 1998.

Stoneburner, Gary, Draft –Rev. A NIST Special Publication 800-XX, Risk Management Guide, February 16, 2001.

Swanson, Marianne and Barbara Guttman, NIST Special Publication 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP), Gaithersburg, MD, National Institute of Standards and Technology, September 20, 1995.

Swanson, Marianne and Federal Computer Security Program Managers' Forum Working Group, NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, Gaithersburg, MD, National Institute of Standards and Technology, December 1998.