**NIST Special Publication 800-18**

# Guide for Developing Security Plans for Information Technology Systems

**Marianne Swanson**

**Federal Computer Security Program Managers' Forum Working Group**

**December 1998**

# Executive Summary

The objective of system security planning is to improve protection of information technology (IT) resources. All federal systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan. The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," and Public Law 100-235, "Computer Security Act of 1987."

The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager. Additional information may be included in the basic plan and the structure and format organized according to agency needs, so long as the major sections described in this document are adequately covered and readily identifiable.

In order for the plans to adequately reflect the protection of the resources, a management official must authorize a system to process information or operate. The authorization of a system to process information, granted by a management official, provides an important quality control. By authorizing processing in a system, the manager accepts its associated risk.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the security plan establishes and documents the security controls, it should form the basis for the authorization, supplemented by more specific studies as needed. In addition, a periodic review of controls should also contribute to future authorizations. Re-authorization should occur prior to a significant change in processing, but at least every three years. It should be done more often where there is a high risk and potential magnitude of harm.

## Table of Contents

## Acknowledgments

The National Institute of Standards and Technology would like to acknowledge the Federal Computer Security Program Managers' Forum, an organization sponsored by the National Institute of Standards and Technology. The Forum established a working group to develop a guideline for developing security plans for all federal systems. This document evolved from that effort. The members of the working group are identified below. Please note that some members' affiliations have changed; however, both individual and agency are acknowledged.

Robert L. Gignilliant (Chairperson)
Department of Health & Human Services

Sadie I. Pitcher (Originating Author)
Department of Commerce, Retired

Daniel Bartko
Department of State

Judy Bloom
Department of Justice

Pauline Bowen
Food and Drug Administration

Marlene Broadus
Department of State

Doris Carter
Department of Labor

Grace Culver
Patent and Trademark Office

Brenda Dyer
Department of Justice

William Gill
Environmental Protection Agency

Alice Gannon
Office of Federal Housing
Enterprise Oversight

John Haines
Department of Interior

W. Ron Hess
National Institutes of Health

Mary Stone Holland
Department of State

Sherman Howell
Federal Deposit Insurance Corporation

Phyllis Jones
Internal Revenue Service

John Kurpiel
General Services Administration

Sonja D. Martin
Agency for International Development

Francis D. McCusker
Patent and Trademark Office

Don McGinnis
Environmental Protection Agency

Louis M. Numkin
Nuclear Regulatory Commission

Steve Posniak
Equal Employment Opportunity
Commission

Lloyd Reese
Department of Veterans Affairs

Bob Sargis
Administration for Children and Families

Phil Sibert
Department of Energy

Steve Skolochenko
Department of Justice

Carl Spellacy
Office of Thrift Supervision

Josephine M. Thomas
Small Business Administration

John Tressler
Department of Education

Timothy Turner
Office of Federal Housing Enterprise Oversight

Rebecca Vasvary
National Oceanographic and Atmospherics Administration

Ted I. Wells
Patent and Trademark Office

Timothy M. Wooten
Farm Credit Administration

In addition, a special thank you is due to Cynthia A. Gosewehr, Census Bureau, for sharing the planning guide template.

Finally, NIST would like to thank all the other individuals who contributed to this effort; their assistance was critical to the preparation of this document.

# 1 Introduction

Today's rapidly changing technical environment requires federal agencies to adopt a minimum set of management controls to protect their information technology (IT) resources. These management controls are directed at individual information technology users in order to reflect the distributed nature of today's technology. Technical and **operational controls** support management controls. To be effective, these controls all must interrelate. This document provides a guideline for federal agencies to follow when developing the security plans that document the management, technical, and operational controls for federal automated information **systems**.

## 1.1 Background

The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," updated in 1996, and of Public Law 100-235, "Computer Security Act of 1987."

OMB Circular A-130, Appendix III, does not distinguish between sensitive and non-sensitive systems. Rather, consistent with the Computer Security Act of 1987, the Circular recognizes that federal automated information systems have varied sensitivity and criticality. All federal systems have some level of sensitivity and require protection as part of good management practice. The generic term "system" is used in this document to mean either a **major application** or a **general support system**.

## 1.2 Major Application or General Support System Plans

All applications and systems must be covered by system security plans if they are categorized as a "major application" or "general support system." Specific security plans for other applications are not required because the security controls for those applications or systems would be provided by the general support systems in which they operate. For example, a department-wide Financial Management System would be a major application requiring its own security plan. A local program designed to track expenditures against an office budget might not be considered a major application and would be covered by a general support system security plan for an office automation system or a local area network (LAN). Standard commercial off-the-shelf software (such as word processing software, electronic mail software, utility software, or other general-purpose software) would not typically be considered a major application and would be covered by the plans for the general support system on which they are installed.

## 1.3 Relationship to Other NIST Security Documents

This document completes the NIST trilogy of IT security program-level guidance. The planning guide is intended to be a companion to NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook* (Handbook) *and* NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* (Principles and Practices). The *NIST Handbook* contains over 200 pages of guidance in securing computer-based resources. The document explains important concepts, cost considerations, and interrelationships of security controls. It provides a broad overview of computer security and provides the "why" to many security-related issues. The *Handbook* served as the template for deriving the practices recommended in the NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*.

The *Principles and Practices* document provides the "what" should be done in securing IT resources. The principles section contains the intrinsic expectations that must be met whether the system is small, large or owned by a government agency or by a private corporation. The practices section is the next level in the foundation of the document. The practices show what should be done to enhance or measure an existing computer security program or to aid in the development of a new program.

This planning guide builds on the practices portion in this document, most practices are further expanded and in some cases, excerpts are provided for clarity. The *NIST Handbook* and the *Principles and Practices* documents should be referenced for further information. The *NIST Handbook* should be used to obtain additional detail or explanation on any of the controls listed. The *Principles and Practices* document should be used as a reference to describe the controls and used as a guide for reviewing the plan. Each planning guide control chapter easily maps to the *NIST Handbook* and the *Principles and Practices* document since the chapters in all three documents are listed under the same three controls, i.e., management, operational, and technical.

The *NIST Handbook* and the *Principles and Practices* documents can be obtained from the NIST Computer Security Resource Clearinghouse Web site at the URL: http://csrc.nist.gov/

## 1.4 Purposes of Security Plans

The purposes of system security plans are to:

- Provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements; and

- Delineate responsibilities and expected behavior of all individuals who access the system.

## 1.5 Security Plan Responsibilities

The System Owner[1] is responsible for ensuring that the security plan is prepared and for implementing the plan and monitoring its effectiveness. Security plans should reflect input from various individuals with responsibilities concerning the system, including functional "end users," Information Owners,[2] the System Administrator, and the System Security Manager.

Agencies may require contractor compliance with this guide as a contract requirement. A security plan in the format specified in this document or in another agreed upon format is suggested in those cases where vendors are operating a system under contract to the federal government. In those instances where a contractor or other entity (e.g., state or local government) operates a system that supports a federal function, a security plan is required.

OMB Circular A-130 requires a summary of the security plan to be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35).

Agencies should develop policy on the security planning process. Security plans are living documents that require periodic reviews, modifications, and milestone or completion dates for planned controls. Procedures should be in place outlining who reviews the plans and follows up on planned controls. In addition, procedures are needed describing how security plans will be used in the authorization for processing process.

## 1.6 Recommended Format

While the format in this guide is recommended, it is recognized that some agencies have developed plans using other formats that meet the A-130 requirements described in this document. This document is intended as guidance only and should not be construed as the only format allowed. A standardized approach, however, not only makes the development of the plan easier by providing examples, but also provides a baseline to review plans. The level of detail included within the plan should be consistent with the criticality and value of the system to the organization's mission (i.e., a more detailed plan is required for systems critical to the organization's mission). The security plan should fully identify and describe the controls currently in place or planned for the system and should include a list of **rules of behavior**.

---

[1] The System Owner is responsible for defining the system's operating parameters, authorized functions, and security requirements. The information owner for information stored within, processed by, or transmitted by a system may or may not be the same as the System Owner. Also, a single system may utilize information from multiple Information Owners.

[2] The Information Owner is responsible for establishing the rules for appropriate use and protection of the subject data/information (rules of behavior). The Information Owner retains that responsibility even when the data/information are shared with other organizations.

## 1.7 Advice and Comment on Plan

Independent advice and comment on the security plan shall be solicited prior to the plan's implementation. Independent advice and comment must be obtained from individuals within or outside the organization, who are not responsible for the system's development, implementation, or operation. Organizational policy should define who will provide the independent advice. Individuals providing advice and comment should be independent of the system owner's reporting chain and should have adequate knowledge or experience to ensure the plan contains appropriate information and meets organizational security policy and standards. Appropriate individuals might include an organization's IT Security Program Manager, IT managers of other systems, outside contractors, or personnel from another federal organization.

## 1.8 Audience

This guide has two distinct uses. It is to be used by those individuals responsible for IT security at the system level and at the organization level. The document is intended as a guide when creating security plans. It is written specifically for individuals with little or no computer security expertise. The document also can be used as an auditing tool by auditors, managers, and IT security officers. The concepts presented are generic and can be applied to organizations in private and public sectors.

## 1.9 Organization of Document

Chapter 1 introduces the document and explains its relationship to other NIST guidance on IT security. Chapter 2 describes the system analysis process. Chapter 3 provides guidance on the general information contained in all security plans. Chapter 4 presents the management controls that should be considered. Chapter 5 describes the operational controls and Chapter 6 presents the **technical controls**. Chapter 5 and Chapter 6 have been split into two formats: one format for major applications and another format for general support systems. Differences between the operational and technical controls of major applications and general support systems warrant separate sections. The formats are depicted by 5.MA and 6.MA for major applications and 5.GSS and 6.GSS for general support systems. Appendix A provides an example of Rules of Behavior for a major application. Appendix B provides an example of Rules of Behavior for a general support system. To assist the reader in preparing the plan with the appropriate format, Appendix C contains two security plan templates, one for major applications and one for general support systems. Appendix D contains a glossary of terms. The terms found in the glossary are highlighted in this document the first time used. Appendix E lists references that may be useful in preparing security plans and finally, an Index is provided for locating specific topics.

# 2 System Analysis

Once completed, a security plan will contain technical information about the system, its security requirements, and the controls implemented to provide protection against its **risks** and vulnerabilities. Before the plan can be developed, a determination must be made as to which type of plan is required for a system. This section walks the reader through an analysis of the system to determine the boundaries of the system and the type of system.

## 2.1 System Boundaries

Defining what constitutes a "system" for the purposes of this guideline requires an analysis of system boundaries and organizational responsibilities. A system, as defined by this guideline, is identified by constructing logical boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a security plan. Each element of the system must:

- 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.

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 for their jobs; and [4] a system with multiple identical configurations that are installed in locations with the same environmental and physical safeguards).

## 2.2 Multiple Similar Systems

An organization may have systems that differ only in the responsible organization or the physical environment in which they are located (e.g., air traffic control systems). In such instances, it is appropriate and recommended to use plans that are identical except for those areas of difference. This approach provides consistent levels of protection for similar systems.

**Example for Multiple Similar Systems**

A general support system in Washington, D.C., provides distributed application and telecommunications support for three remote sites located in California, Colorado, and Alaska. A separate security plan may be prepared for each location (a total of four plans) or a single plan may be prepared with abbreviated, subordinate plans for each remote site. Specifically, a "master plan" would be developed for the Washington, D.C., site by the organization that has responsibility for system development, operation, and maintenance. Remote site security plans would be a shorter "system site plan" that references the security plan for the Washington, D.C., system (using its unique name identifier) and that contains information unique to the site (e.g., physical, environmental, responsible individuals, hardware, contingency plan, risk assessment, authorization for processing, and milestone or completion dates for planned controls). System plans that reference the master plan must also be listed in the master plan by their unique name identifiers.

This approach facilitates analysis of the security provided to the entire distributed system and helps ensure that there are no weak security links.

## 2.3 System Category

The next step is to categorize each system as either a "**major application**" or as a "**general support system.**" All applications should be covered by a security plan. The applications will either be covered individually if they have been designated as a major application or within the security plan of a general support system. A system may be designated as a major application even though it is also supported by a system that has been designated as a general support system. For example, a LAN may be designated a general support system and have a security plan. The organization's accounting system may be designated as a major application even though it is supported by the computing and communication resources of the LAN. In this example, the major application requires additional security requirements due to the sensitivity of the information the application processes. When a security plan is required for a major application that is supported by a general support system, coordination of both plans is required.

### 2.3.1 Major Applications

All federal applications have value and require some level of protection. Certain applications, because of the information they contain, process, or transmit or because of their criticality to the organization's missions, require special management oversight. These applications are major applications.

Agencies are expected to exercise management judgment in determining which of their applications are major applications and to ensure that the security requirements of non-major applications are discussed as part of the security plan for the applicable general support systems.

Major applications are systems that perform clearly defined functions for which there are readily identifiable security considerations and needs (e.g., an electronic funds transfer system). A major application might comprise many individual programs and hardware, software, and telecommunications components. These components can be a single software application or a combination of hardware/software focused on supporting a specific mission-related function. A major application may also consist of multiple individual applications if all are related to a single mission function (e.g., payroll or personnel). If a system is defined as a major application and the application is run on another organization's general support system:

- Notify the system owner that the application is critical or contains **sensitive information** and provide specific security requirements;
- Provide a copy of the major application's security plan to the operator of the general support system;
- Request a copy of the system security plan of the general support system and ensure it provides adequate protection for the application and information; and
- Include a reference to the general support system security plan, including the unique name/identifier information in Section 3.5, System Environment.

### 2.3.2 General Support System

A general support system is interconnected information resources under the same direct management control which shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example, can be a:

- LAN including smart terminals that support a branch office;
- Backbone (e.g., agency-wide);
- Communications network;
- Departmental data processing center including its operating system and utilities,
- Tactical radio network; or

- Shared information processing service organization.

A major application can run on a general support system. The general support system plan should reference the major application plan(s) in Section 3.4, General Description/Purpose.

# 3 Plan Development – All Systems

The remainder of this document guides the reader in writing a security plan. This section provides and requires general information that applies to all systems. Note: A template of all sections contained in a security plan is provided in Appendix C. The template is separated into two formats, one for major applications and one for general support systems.

## 3.1 Plan Control

All security plans, at a minimum, should be marked, handled, and controlled to the level of sensitivity determined by organizational policy. In addition, all security plans should be dated for ease of tracking modifications and approvals. Dating each page of a security plan may be appropriate if updates are to be made through change pages. All plans begin with the following system identification section.

## 3.2 System Identification

The first section of the plan provides basic identifying information about the system. Both types of plans must contain general descriptive information regarding who is responsible for the system, the purpose of the system, and the **sensitivity** level of the system.

### 3.2.1 System Name/Title

The plan begins with listing the name and title of the system/application. Each system/application 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 identifier could be a combination of alphabetic and numeric characters and can be used in combination with the system/application name. 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. Note: If no unique name/identifier has been assigned or is not known, contact the security or information resource management office for assistance.

### 3.2.2 Responsible Organization

In this section, list the federal organizational sub-component responsible for the system. If a state or local government or contractor performs the function, identify both the federal and other organization and describe the relationship. Be specific about the organization and do not abbreviate. Include physical locations and addresses.

**Example of Responsible Organization**

Department of Federal Government
Office of the Secretary
Information Resources Management
14th Street and Constitution Avenue, Room 1000
Washington, DC 20000

This system is maintained by:

Contractor Firm
163 Main Street, Suite 202
Washington, DC 20000

### 3.2.3 Information Contact(s)

List the name, title, organization, and telephone number of one or more persons designated to be the point(s) of contact for this system. One of the contacts given should be identified as the system owner. The designated persons should have sufficient knowledge of the system to be able to provide additional information or points of contact, as needed.

**Example Information Contacts**

Ms. Jane Smith (System Owner)
ABC Division Chief
1111 West Street, Room 222
Rockville, MD 20852
(301) 123-4567

Mr. John Doe
Program Manager
ABC Division
1111 West Street, Room 233
Rockville, MD 20852
(301) 123-8910

### 3.2.4 Assignment of Security Responsibility

An individual must be assigned responsibility in writing to ensure that the application or general support system has adequate security. To be effective, this individual must be knowledgeable of the management, operational, and technical controls used to protect the system.

Include the name, title, and telephone number of the individual who has been assigned responsibility for the security of the system.

**Example Security Contact**

Bill Smith,
Computer Specialist
ABC Division, XYZ Branch
1111 West Street, Room 444
Rockville, MD 20852
(301) 123-1213

## 3.3 System Operational Status

Indicate one or more of the following for the **system's operational status**. If more than one status is selected, list which part of the system is covered under each status.

- *Operational* — the system is operating.
- *Under development* — the system is being designed, developed, or implemented.
- *Undergoing a major modification* — the system is undergoing a major conversion or transition.

If the system is under development or undergoing a major modification, provide information about the methods used to assure that up-front security requirements are included. Include specific controls in the appropriate sections of the plan depending on where the system is in the security life cycle.

## 3.4 General Description/Purpose

Present a brief description (one-three paragraphs) of the function and purpose of the system (e.g., economic indicator, network support for an organization, business census data analysis, crop reporting support).

If the system is a general support system, list all applications supported by the general support system. Specify if the application is or is not a major application and include unique name/identifiers, where applicable. Describe each application's function and the information processed. Include a list of user organizations, whether they are internal or external to the system owner's organization, and a general description of the type of information and processing provided. Request information from the application owners (and a copy of the security plans for major applications) to ensure their requirements are met.

## 3.5 System Environment

Provide a brief (one-three paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as:

- The system is connected to the Internet;
- It is located in a harsh or overseas environment;
- Software is rapidly implemented;
- The software resides on an open network used by the general public or with overseas access;
- The application is processed at a facility outside of the organization's control; or
- The general support mainframe has dial-up lines.

**Example System Environment**

The system is physically housed in a government-owned building located in Washington, D.C. The entire building is occupied by Department of ABC Civil Service and contractor personnel and is not open to the general public. The system uses mainframe hardware. The system consists of a Brand X 9999 supercomputer and a Brand Y 8888 mainframe configuration. The operating system running on the Brand X 9999 system is OS-YYYY and on the Brand Y 8888 system is OS-OOOO1. The security software protecting all system resources from the top levels are XYZ and PDQ. DOA-XX-0123, a complex, wide-area communication network system, provides support to client agencies nationwide.

Describe the primary computing platform(s) used (e.g., mainframe, desk top, LAN or Wide Area Network (WAN). Include a general description of the principal system components, including hardware, software, and communications resources. Discuss the type of communications included (e.g., dedicated circuits, dial circuits, public data/voice **networks**, Internet). Describe controls used to protect communication lines in the appropriate sections of the security plan.

Include any security software protecting the system and information. Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented or are planned, rather than listing the controls that are available in the software. Controls that are available, but not implemented, provide no protection.

## 3.6 System Interconnection/Information Sharing

System interconnection is the direct connection of systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection and information sharing and the increased controls required to mitigate those vulnerabilities. The security plan for the systems often serves as a mechanism to effect this security information exchange and allows management to make informed decisions regarding risk reduction and acceptance.

OMB Circular A-130 requires that written management authorization (often in the form of a Memorandum of Understanding or Agreement,) be obtained prior to connecting with other systems and/or sharing sensitive data/information. The written authorization shall detail the rules of behavior and controls that must be maintained by the interconnecting systems. A description of the rules for interconnecting systems and for protecting shared data must be included with this security plan. See Section 4.3, Rules of Behavior.

In this section, provide the following information concerning the authorization for the connection to other systems or the sharing of information:

- List of interconnected systems (including Internet);
- Unique system identifiers, if appropriate;
- Name of system(s);
- Organization owning the other system(s);

- Type of interconnection (TCP/IP, Dial, SNA, etc.);
- Short discussion of major concerns or considerations in determining interconnection (do not repeat the system rules included in Section 4.3);
- Name and title of authorizing management official(s);
- Date of authorization;
- System of Record, if applicable (Privacy Act data);
- Sensitivity level of each system;
- Interaction among systems; and
- Security concerns and Rules of Behavior of the other systems that need to be considered in the protection of this system.

## 3.7 Sensitivity of Information Handled

This section provides a description of the types of information handled by the system and an analysis of the criticality of the information. The sensitivity and criticality of the information stored within, processed by, or transmitted by a system provides a basis for the value of the system and is one of the major factors in **risk management**. The description will provide information to a variety of users, including:

- Analysts/programmers who will use it to help design appropriate security controls;
- Internal and external auditors evaluating system security measures; and
- Managers making decisions about the reasonableness of security countermeasures.

The nature of the information sensitivity and criticality must be described in this section. The description must contain information on applicable laws, regulations, and policies affecting the system and a general description of sensitivity as discussed below.

### 3.7.1 Laws, Regulations, and Policies Affecting the System

List any laws, regulations, or policies that establish specific requirements for **confidentiality**, **integrity**, or **availability** of data/information in the system. The Computer Security Act of 1987, OMB Circular A-130, and general agency security requirements need not be listed since they mandate security for all systems. Each organization should decide on the level of laws, regulations, and policies to include in the

security plan. Examples might include the Privacy Act or a specific statute or regulation concerning the information processed (e.g., tax or census information). If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) are used for computer matching activities.

See Appendix E for reference to the NIST Computer Security Division's Computer Security Resource Clearinghouse (CSRC) Web site. CSRC contains information on a wide variety of computer security resources, including a list of applicable laws and regulations.

**Example Applicable Laws or Regulations Affecting the System**

Privacy Act of 1974 (PL-93-579)
Paperwork Reduction Act of 1980 as amended in 1995
OMB Circular A-123

### 3.7.2 General Description of Sensitivity

Both information and information systems have distinct life cycles. It is important that the degree of sensitivity of information be assessed by considering the requirements for **availability, integrity, and confidentiality** of the information. This process should occur at the beginning of the information system's life cycle and be re-examined during each life cycle stage.

The integration of security considerations early in the life cycle avoids costly retrofitting of safeguards. However, security requirements can be incorporated during any life cycle stage. The purpose of this section is to review the system requirements against the need for availability, integrity, and confidentiality. By performing this analysis, the value of the system can be determined. The value is one of the first major factors in risk management. A system may need protection for one or more of the following reasons:

- *Confidentiality*

The system contains information that requires protection from unauthorized disclosure.

**Example of Information Requiring Protection — Confidentiality**

Timed dissemination information (e.g., crop report information), personal information (covered by Privacy Act), proprietary business information (e.g., business plans).

- *Integrity*

The system contains information which must be protected from unauthorized, unanticipated, or unintentional modification.

**Example of Information Requiring Protection — Integrity**

Census information, economic indicators, or financial transaction systems.

- *Availability*

The system contains information or provides services which must be available on a timely basis to meet mission requirements or to avoid substantial losses.

**Example of Information Requiring Protection — Availability**

Systems critical to safety, life support, and hurricane forecasting.

Describe, in general terms, the information handled by the system and the need for protective measures. Relate the information handled to each of the three basic protection requirements above (**confidentiality**, **integrity**, and **availability**). Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system. To the extent possible, describe this impact in terms of cost, inability to carry out mandated functions, timeliness, etc.

For each of the three categories (**confidentiality**, **integrity**, and **availability**), indicate if the protection requirement is:

- *High* — a critical concern of the system;

- *Medium*— an important concern, but not necessarily paramount in the organization's priorities; or

- *Low* — some minimal level or security is required, but not to the same degree as the previous two categories.

### Examples of a General Protection Requirement Statement

A high degree of security for the system is considered mandatory to protect the confidentiality, integrity, and availability of information. The protection requirements for all applications are critical concerns for the system.

**or**

Confidentiality is not a concern for this system as it contains information intended for immediate release to the general public concerning severe storms. The integrity of the information, however, is extremely important to ensure that the most accurate information is provided to the public to allow them to make decisions about the safety of their families and property. The most critical concern is to ensure that the system is available at all times to acquire, process, and provide warning information immediately about life-threatening storms.

| Example Confidentiality Considerations | |
|---|---|
| **Evaluation** | **Comment** |
| **High** | The application contains proprietary business information and other financial information, which if disclosed to unauthorized sources, could cause unfair advantage for vendors, contractors, or individuals and could result in financial loss or adverse legal action to user organizations. |
| **Medium** | Security requirements for assuring confidentiality are of moderate importance. Having access to only small portions of the information has little practical purpose and the satellite imagery data does not reveal information involving national security. |
| **Low** | The mission of this system is to produce local weather forecast information that is made available to the news media forecasters and the general public at all times. None of the information requires protection against disclosure. |

| Example Integrity Considerations | |
|---|---|
| **Evaluation** | **Comment** |
| **High** | The application is a financial transaction system. Unauthorized or unintentional modification of this information could result in fraud, under or over payments of obligations, fines, or penalties resulting from late or inadequate payments, and loss of public confidence. |
| **Medium** | Assurance of the integrity of the information is required to the extent that destruction of the information would require significant expenditures of time and effort to replace. Although corrupted information would present an inconvenience to the staff, most information, and all vital information, is backed up by either paper documentation or on disk. |
| **Low** | The system mainly contains messages and reports. If these messages and reports were modified by unauthorized, unanticipated or unintentional means, employees would detect the modifications; however, these modifications would not be a major concern for the organization. |

| Example Availability Considerations | |
|---|---|
| **Evaluation** | **Comment** |
| **High** | The application contains personnel and payroll information concerning employees of the various user groups. Unavailability of the system could result in inability to meet payroll obligations and could cause work stoppage and failure of user organizations to meet critical mission requirements. The system requires 24-hour access. |
| **Medium** | Information availability is of moderate concern to the mission. Macintosh and IBM PC availability would be required within the four to five-day range. Information backups maintained at off-site storage would be sufficient to carry on with limited office tasks. |
| **Low** | The system serves primarily as a server for e-mail for the seven users of the system. Conference messages are duplicated between Seattle and D.C. servers. Should the system become unavailable, the D.C. users would connect to the Seattle server and continue to work with only the loss of old mail messages. |

# 4 Management Controls

In this section, describe the management control measures (**in place** or **planned**) that are intended to meet the protection requirements of the major application or general support system. Management controls focus on the management of the computer security system and the management of risk for a system. The types of control measures shall be consistent with the need for protection of the major application or general support system. To aid the reader, a brief explanation of the various management controls is provided. For more detail on management controls, see NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook.*

## 4.1 Risk Assessment and Management

OMB Circular A-130 no longer requires the preparation of a formal risk analysis. It does, however, require an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system. The methods used to assess the nature and level of risk to the system should include a consideration of the major factors in risk management: the value of the system or application, **threats**, vulnerabilities, and the effectiveness of current or proposed safeguards. The methods used should be described in at least one paragraph. For example, did the selected risk assessment methodology identify threats, vulnerabilities, and the additional security measures required to mitigate or eliminate the potential that those threats/vulnerabilities could have on the system or its assets? Include the date that the system risk assessment was conducted. State how the identified risks relate to the requirements for confidentiality, integrity, and availability determined for the system.

If there is no risk assessment for your system, include a milestone date (month and year) for completion of the risk assessment. If the risk assessment is more than three years old or there have been major changes to the system or functions, include a milestone date (month and year) for completion of a new or updated risk assessment. Assessing the risk to a system should be an ongoing activity to ensure that new threats and vulnerabilities are identified and appropriate security measures are implemented.

## 4.2 Review of Security Controls

OMB Circular A-130 requires that at least every three years an independent review of the security controls for each major application be performed. For general support systems, OMB Circular A-130 requires that the security controls be reviewed by an independent audit or self review at least every three years. Describe the type of review and findings conducted on the general support system or major application in the last three years. Include information about the last independent audit or review of the system and who conducted the review. Discuss any findings or recommendations from the review and include information concerning correction of any deficiencies or completion of any recommendations. Indicate if the review identified a deficiency reportable under OMB

Circular No. A-123 or the Federal Managers' Financial Integrity Act if there is no assignment of security responsibility, no security plan, or no authorization to process for a system. Indicate in this section if an independent audit or review has not been conducted on this system.

Security reviews, assessments, or evaluations may be conducted on your system by internal or external organizations or groups. Such reviews include ones conducted on your facility or site by physical security specialists from other components of your organization, system audits, or security program reviews performed by your Inspector General's staff or contractors. These reviews may evaluate the security of the total system or a logical segment/subsystem. The system descriptions, findings, and recommendations from these types of reviews may serve as the independent review, if the review is thorough, and may provide information to support your risk assessment and risk management. If other types of security evaluations have been conducted on your system, include information about who performed the review, when the review was performed, the purpose of the review, the findings, and the actions taken as a result of the review.

The review or audit should be independent of the manager responsible for the major application or general support system. Independent audits can be internal or external but should be performed by an individual or organization free from personal and external factors which could impair their independence or their perceived independence (e.g., they designed the system under review). For some high-risk systems with rapidly changing technology, three years may be too long and reviews may need to be conducted more frequently. The objective of these reviews is to provide verification that the controls selected and/or installed provide a level of protection commensurate with the acceptable level of risk for the system. The determination that the level of risk is acceptable must be made relative to the system requirements for confidentiality, integrity, and availability as well as the identified threats.

The security of a system may degrade over time, as the technology changes, the system evolves, or people and procedures change. Periodic reviews provide assurance that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection.

The type and rigor of review or audit should be commensurate with the acceptable level of risk that is established in the rules for the system and the likelihood of learning useful information to improve security. Technical tools such as virus scanners, **vulnerability** assessment products (which look for known security problems, configuration errors, and the installation of the latest hardware/software “patches”), and penetration testing can assist in the ongoing review of system security measures. These tools, however, are no substitute for a formal management review at least every three years.

## 4.3 Rules of Behavior

Attach the rules of behavior for the general support system or major application as an appendix and reference the appendix number in this section, or insert the rules into this section. A set of rules of behavior must be established for each system. The security required by the rules is only as stringent as necessary to provide adequate security for the system and the information it contains. The acceptable level of risk should form the basis for determining the rules. Appendix A contains a sample rules of behavior for a financial system, which is categorized as a major application. Appendix B contains a sample rules of behavior for a local area network, which is categorized as a general support system.

The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules should state the consequences of inconsistent behavior or noncompliance. The rules should be in writing and form the basis for security awareness and training.

Rules of Behavior shall also include appropriate limits on interconnections to other systems and define service provision and restoration priorities. They should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and **individual accountability**. Rules should reflect administrative and technical security controls in the system. For example, rules regarding password use should be consistent with technical password features in the system. Such rules would also include limitations on changing information, searching databases, or divulging information. Rules of behavior may be enforced through administrative sanctions specifically related to the system (e.g., loss of system privileges) or through more general sanctions as are imposed for violating other rules of conduct.

The rules of behavior should be made available to every user prior to receiving authorization for access to the system. It is recommended that the rules contain a signature page for each user to acknowledge receipt.

## 4.4 Planning for Security in the Life Cycle

Although a computer security plan can be developed for a system at any point in the life cycle, the recommended approach is to draw up the plan at the beginning of the computer system life cycle. It is recognized that in some cases, the system may at any one time be in several phases of the life cycle. For example, a large human resources system may be in the operation/maintenance phase, while the older, batch-oriented, input sub-system is being replaced by a new, distributed, interactive user interface. In this case, the life cycle phases for the system are the disposal phase (data and equipment) related to the retirement of the batch-oriented transaction system, the initiation and acquisition phase associated with the replacement interactive input system, and the operations/maintenance phase for the balance of the system.

In this section, determine which phase(s) of the life cycle the system, or parts of the system, are in. Identify how security has been handled during the applicable life cycle

phase. Listed below is a description of each phase of the life cycle, which includes questions that will prompt the reader to identify how security has been addressed during the life cycle phase(s) that the major application or general support system is in. There are many models for the IT system life cycle but most contain five basic phases: Initiation, development/acquisition, implementation, operation, and disposal.

### 4.4.1 Initiation Phase

During the initiation phase, the need for a system is expressed and the purpose of the system is documented. A sensitivity assessment can be performed which looks at the sensitivity of the information to be processed and the system itself. If the system or part of the system is in the initiation phase, reference the sensitivity assessment described in Section 3.7, Sensitivity of Information Handled.

### 4.4.2 Development/Acquisition Phase

During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle.

During the first part of the development/acquisition phase, security requirements should be developed at the same time system planners define the requirements of the system. These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., background checks for system developers), or operational practices (e.g., awareness and training). If the system or part of the system is in this phase, include a general description of any specifications that were used and whether they are being maintained. Among the questions that should be addressed are the following:

- During the system design, were security requirements identified?
- Were the appropriate security controls with associated evaluation and test procedures developed before the procurement action?
- Did the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?
- Did the requirements permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented?
- If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security requirements identified and included in the acquisition specifications?

### 4.4.3 Implementation Phase

In the implementation phase, the system's security features should be configured and enabled, the system should be tested and installed or fielded, and the system authorized for processing. (See Section 4.5, Authorize Processing, for a description of that requirement.) A design review and systems test should be performed prior to placing the system into operation to assure that it meets security specifications. In addition, if new controls are added to the application or the support system, additional acceptance tests of those new controls must be performed. This ensures that new controls meet security specifications and do not conflict with or invalidate existing controls. The results of the design reviews and system tests should be fully documented, updated as new reviews or tests are performed, and maintained in the official organization records.

If the system or parts of the system are in the implementation phase, describe when and who conducted the design reviews and systems tests. Include information about additional design reviews and systems tests for any new controls added after the initial acceptance tests were completed. Discuss whether the documentation of these reviews and tests have been kept up-to-date and maintained in the organization records.

### 4.4.4 Operation/Maintenance Phase

During this phase, the system performs its work. The system is almost always being continuously modified by the addition of hardware and software and by numerous other events. If the system is undergoing modifications, determine which phase of the life cycle the system modifications are in and describe the security activities conducted or planned for in that part of the system. For the system in the operation/maintenance phase, the security plan documents the security activities. In appropriate sections of this security plan, the following high-level items should be described:

- Security Operations and Administration. Operation of a system involves many security activities. Performing backups, holding training classes, managing cryptographic keys, keeping up with user administration and access privileges, and updating security software are some examples.

- Operational Assurance. Operational assurance examines whether a system is operated according to its current security requirements. This includes both the actions of people who operate or use the system and the functioning of technical controls. A management official must authorize in writing the use of the system based on implementation of its security plan. (See Section 4.5, Authorize Processing for a description of that requirement.)

- Audits and Monitoring. To maintain operational assurance, organizations use two basic methods: system audits and monitoring. These terms are used loosely within the computer security community and often overlap. A system audit is a one-time or periodic event to evaluate security. Monitoring refers to an ongoing activity that examines either the system or the users. In general, the more "real-time" an activity is, the more it falls into the category of monitoring.

### 4.4.5 Disposal Phase

The disposal phase of the IT system life cycle involves the disposition of information, hardware, and software. If the system or part of the system is at the end of the life cycle, briefly describe in this section how the following items are disposed:

- Information. Information may be moved to another system, archived, discarded, or destroyed. When archiving information, consider the method for retrieving the information in the future. While electronic information is generally easier to retrieve and store, the technology used to create the records may not be readily available in the future. Measures may also have to be taken for the future use of data that has been encrypted, such as taking appropriate steps to ensure the secure long-term storage of cryptographic keys. It is important to consider legal requirements for records retention when disposing of IT systems. For federal systems, system management officials should consult with their office responsible for retaining and archiving federal records.

- Media Sanitization. The removal of information from a storage medium (such as a hard disk or tape) is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by keyboard attack) and purging (rendering information unrecoverable against laboratory attack). There are three general methods of purging media: overwriting, degaussing (for magnetic media only), and destruction.

## 4.5 Authorize Processing

The term “authorize processing” is the authorization granted by a management official for a system to process information. (Note: Some agencies refer to this authorization as **accreditation**.) Authorization provides a form of quality control and is required under OMB Circular A-130. It forces managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. By authorizing processing in a system, a manager accepts the risk associated with it. In this section of the plan, include the date of authorization, name, and title of management official. If not authorized, provide the name and title of manager requesting approval to operate and date of request.

Both the security official and the authorizing management official have security responsibilities. The security official is closer to the day-to-day operation of the system and will direct, perform, or monitor security tasks. The authorizing official will normally have general responsibility for the organization supported by the system. Authorization is not a decision that should be made by the security staff. Some agencies have established the system approval process as a formal accreditation procedure where the approving authority is termed the Designated Approving/Accreditation Authority (DAA). Formalization of the system authorization process reduces the potential that systems will be placed into a production environment without appropriate management review.

Management authorization must be based on an assessment of management, operational, and technical controls. Since the security plan establishes the system protection requirements and documents the security controls in the system, it should form the basis for the authorization. Authorization is usually supported by a technical evaluation and/or security evaluation, risk assessment, contingency plan, and signed rules of behavior. Note: Some agencies refer to the technical evaluation and/or security evaluation as a certification review. Re-authorization should occur prior to a significant change in the system, but at least every three years. It should be done more often where there is high risk and potential magnitude of harm.

Below is the minimum security controls that must be in place prior to authorizing a system for processing. The level of controls should be consistent with the level of sensitivity the system contains.

- Technical and/or security evaluation complete.
- Risk assessment conducted.
- Rules of behavior established and signed by users.
- Contingency plan developed and tested.
- Security plan developed, updated, and reviewed.
- System meets all applicable federal laws, regulations, policies, guidelines, and standards.
- In-place and planned security safeguards appear to be adequate and appropriate for the system.
- In-place safeguards are operating as intended.

# 5 Operational Controls

Beginning in this chapter and continuing through Chapter 6, Technical Controls, there are two formats and related guidance provided: one format and related guidance for major applications and another set for general support systems. From this chapter on, there is enough of a difference between the controls for a major application and a general support system to warrant a division by system type. The section numbering of these two chapters differs from the rest of the document. The two chapters are numbered as 5.MA and 6.MA for Major Application, then 5.GSS and 6.GSS for General Support System.

A template of all sections contained in a security plan is provided in Appendix C. The template is separated into two formats, one for Major Applications and another for General Support Systems.

# 5.MA. Major Application – Operational Controls

The operational controls address security methods that focus on mechanisms that primarily are 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. In this section, describe the operational control measures (**in place** or **planned**) that are intended to meet the protection requirements of the major application.

## 5.MA.1 Personnel Security

The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. All too often, systems experience disruption, damage, loss, or other adverse impact due to the well-intentioned actions of individuals authorized to use or maintain a system (e.g., the programmer who inserts one minor change, then installs the program into the production environment without testing).

In this section, include detailed information about the following personnel security measures. It is recommended that most of these measures be included as part of the Rules of Behavior. If they are incorporated in the Rules of Behavior, reference the applicable section.

- Have all positions been reviewed for sensitivity level? If all positions have not been reviewed, state the planned date for completion of position sensitivity analysis.

- A statement as to whether individuals have received the background screening appropriate for the position to which they are assigned. If all individuals have not had appropriate background screening, include the date by which such screening will be completed.

- If individuals are permitted system access prior to completion of appropriate background screening, describe the conditions under which this is allowed and any compensating controls to mitigate the associated risk.

- Is user access restricted (least privilege) to data files, to processing capability, or to peripherals and type of access (e.g., read, write, execute, delete) to the minimum necessary to perform the job?

- Are critical functions divided among different individuals (separation of duties) to ensure that no individual has all necessary authority or information access which could result in fraudulent activity?

- Is there a process for requesting, establishing, issuing, and closing user accounts?

- What mechanisms are in place for holding users responsible for their actions?

- What are the termination procedures for a friendly termination and an unfriendly termination?

## 5.MA.2 Physical and Environmental Protection

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical and environmental security program should address the following seven topics which are explained below. In this section, briefly describe the physical and environmental controls in place for the major application

### 5.MA.2.1 Explanation of Physical and Environment Security

Access Controls. Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a local area network (LAN) server. Physical access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation. It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied.

Fire Safety Factors. Building fires are a particularly important security threat because of the potential for complete destruction of both hardware and data, the risk to human life, and the pervasiveness of the damage. Smoke, corrosive gases, and high humidity from a localized fire can damage systems throughout an entire building. Consequently, it is important to evaluate the fire safety of buildings that house systems.

Failure of Supporting Utilities. Systems and the people who operate them need to have a reasonably well-controlled operating environment. Consequently, failures of electric power, heating and air-conditioning systems, water, sewage, and other utilities will usually cause a service interruption and may damage hardware. Organizations should ensure that these utilities, including their many elements, function properly.

Structural Collapse. Organizations should be aware that a building may be subjected to a load greater than it can support. Most commonly this results from an earthquake, a snow load on the roof beyond design criteria, an explosion that displaces or cuts structural members, or a fire that weakens structural members.
Plumbing Leaks. While plumbing leaks do not occur every day, they can be seriously disruptive. An organization should know the location of plumbing lines that might

endanger system hardware and take steps to reduce risk (e.g., moving hardware, relocating plumbing lines, and identifying shutoff valves.)

Interception of Data. Depending on the type of data a system processes, there may be a significant risk if the data is intercepted. Organizations should be aware that there are three routes of data interception: direct observation, interception of data transmission, and electromagnetic interception.

Mobile and Portable Systems. The analysis and management of risk usually has to be modified if a system is installed in a vehicle or is portable, such as a laptop computer. The system in a vehicle will share the risks of the vehicle, including accidents and theft, as well as regional and local risks. Organizations should:

- Securely store laptop computers when they are not in use; and

- Encrypt data files on stored media, when cost-effective, as a precaution against disclosure of information if a laptop computer is lost or stolen.

### 5.MA.2.2 Computer Room Example

Appropriate and adequate controls will vary depending on the individual system requirements. The example list shows the types of controls for an application residing on a system in a computer room. The list is not intended to be all-inclusive or to imply that all systems should have all controls listed.

**Example Physical/Environmental Controls For Computer Room**

**In Place**
Card keys for building and work-area entrances
Twenty-four hour guards at all entrances/exits
Cipher lock on computer room door
Raised floor in computer room
Dedicated cooling system
Humidifier in tape library
Emergency lighting in computer room
Four fire extinguishers rated for electrical fires
One B/C-rated fire extinguisher
Smoke, water, and heat detectors
Emergency power-off switch by exit door
Surge suppressor
Emergency replacement server
Zoned dry pipe sprinkler system
Uninterruptable power supply for LAN servers
Power strips/suppressors for peripherals
Power strips/suppressors for computers
Controlled access to file server room

**Planned**
Plastic sheets for water protection, August 1999
Closed-circuit television monitors, January 2000

## 5.MA.3 Production, Input/Output Controls

In this section, provide a synopsis of the procedures in place that support the operations of the application. Below is a sampling of topics that should be reported.

- User support. Is there a help desk or group that offers advice and can respond to security incidents in a timely manner? Are there procedures in place documenting

how to recognize, handle, and report incidents and/or problems? Additional questions are provided in Section 5.GSS.8, Incident Response Capability.

- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.
- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media.
- Audit trails for receipt of sensitive inputs/outputs.
- Procedures for restricting access to output products.
- Procedures and controls used for transporting or mailing media or printed output.
- Internal/external labeling for appropriate sensitivity (e.g., Privacy Act, Proprietary).
- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates).
- Audit trails for inventory management.
- Media storage vault or library physical and environmental protection controls and procedures.
- Procedures for sanitizing electronic media for reuse (e.g., overwrite or degaussing of electronic media).
- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse.
- Procedures for shredding or other destructive measures for hardcopy media when no longer required.

## 5.MA.4 Contingency Planning

Procedures are required that will permit the organization to continue essential functions if information technology support is interrupted. These procedures (contingency plans, business interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated.

Briefly describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable and

provide the detailed plans as an attachment. Include consideration of the following questions in this description:

- Are tested contingency plans in place to permit continuity of mission-critical functions in the event of a catastrophic event?
- Are tested disaster recovery plans in place for all supporting IT systems and networks?
- Are formal written emergency operating procedures posted or located to facilitate their use in emergency situations?
- How often are contingency, disaster, and emergency plans tested?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

Include descriptions of the following controls:

- Any agreements for backup processing (e.g., hotsite contract with a commercial service provider).
- Documented backup procedures including frequency (daily, weekly, monthly) and scope (full backup, incremental backup, and differential backup).
- Location of stored backups (off-site or on-site).
- Generations of backups kept.
- Coverage of backup procedures, e.g., what is being backed up.

## 5.MA.5 Application Software Maintenance Controls

These controls are used to monitor the installation of, and updates to, application software to ensure that the software functions as expected and that a historical record is maintained of application changes. This helps ensure that only authorized software is installed on the system. Such controls may include a software configuration policy that grants managerial approval (re-**authorize processing**) to modifications and requires that changes be documented. Other controls include products and procedures used in auditing for or preventing illegal use of shareware or copyrighted software. Software maintenance procedures may also be termed version control, change management, or configuration management. The following questions are examples of items that should be addressed in responding to this section:

- Was the application software developed in-house or under contract?
- Does the government own the software?
- Was the application software received from another federal agency with the understanding that it is federal government property?
- Is the application software a copyrighted commercial off-the-self product or shareware?
- If a copyrighted commercial off-the-self product (or shareware), were sufficient licensed copies of the software purchased for all of the systems on which this application will be processed?
- Is there a formal change control process in place for the application, and if so, does it require that all changes to the application software be tested and approved before being put into production?
- Are test data "live" data or made-up data?
- Are all changes to the application software documented?
- Have trap door "hot keys" been activated for emergency data repairs?
- Are test results documented?
- How are emergency fixes handled?
- Are there organizational policies against illegal use of copyrighted software or shareware?
- Are periodic audits conducted of users' computers (PCs) to ensure only legal licensed copies of software are installed?
- What products and procedures are used to protect against illegal use of software?
- Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?

## 5.MA.6 Data Integrity/Validation Controls

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements.

In this section, describe any controls that provide assurance to users that the information has not been altered and that the system functions as expected. The following questions are examples of some of the controls that fit in this category:

- Is virus detection and elimination software installed? If so, are there procedures for:
  - Updating virus signature files;
  - Automatic and/or manual virus scans (automatic scan on network log-in, automatic scan on client/server power on, automatic scan on diskette insertion, automatic scan on download from an unprotected source such as the Internet, scan for macro viruses); and
  - Virus eradication and reporting?
- Are reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Are password crackers/checkers used?
- Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? Techniques include consistency and reasonableness checks and validation during data entry and processing. Describe the integrity controls used within the system.
- Are intrusion detection tools installed on the system? Describe where the tool(s) are placed, the type of processes detected/reported, and the procedures for handling intrusions. (Reference Section 5.MA.3 Production, Input/Output Controls if the procedures for handling intrusions are already described.)
- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?
- Is penetration testing performed on the system? If so, what procedures are in place to ensure they are conducted appropriately?
- Is message authentication used in the application to ensure that the sender of a message is known and that the message has not been altered during transmission?

State whether message authentication has been determined to be appropriate for your system. If so, describe the methodology.

## 5.MA.7 Documentation

Documentation is a security control in that it explains how software/hardware is to be used and formalizes security and operational procedures specific to the system. Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security in the application and the support system(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures.

Documentation should be coordinated with the general support system and/or network manager(s) to ensure that adequate application and installation documentation are maintained to provide continuity of operations

List the documentation maintained for the application. The example list is provided to show the type of documentation that would normally be maintained for a system and is not intended to be all inclusive or imply that all systems should have all items listed.

**Example Documentation for Major Application**

- Vendor-supplied documentation of hardware
- Vendor-supplied documentation of software
- Application requirements
- Application security plan
- General support system(s) security plan(s)
- Application program documentation and specifications
- Testing procedures and results
- Standard operating procedures
- Emergency procedures
- Contingency plans
- Memoranda of understanding with interfacing systems
- Disaster recovery plans
- User rules of behavior
- User manuals
- Risk assessment
- Backup procedures
- Authorize processing documents and statement

## 5.MA.8 Security Awareness and Training

The Computer Security Act requires federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practices for all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of the federal agency. This includes contractors as well as employees of the agency. OMB Circular A-130, Appendix III, issued in 1996, enforces such mandatory training by requiring its completion prior to granting access to the system and through periodic refresher training for continued access. Therefore, each user must be versed in acceptable rules of behavior for the application before being allowed access to the system. The training program should also inform the user on how to get help when having difficulty using the system and procedures for reporting security incidents.

Access provided to members of the public should be constrained by controls in the applications, and training should be within the context of those controls and may consist only of notification at the time of access.

Include in this section of the plan information about the following:

- The awareness program for the application (posters, booklets, and trinkets).
- The type and frequency of application-specific training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the-job training).
- The type and frequency of general support system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the-job training).
- The procedures for assuring that employees and contractor personnel have been provided adequate training.

**Note:** Contractor employees are required to receive the same level of automated information systems security awareness and training as federal employees. This training requirement should be included as appropriate in all contracts.

# 6.MA Major Application - Technical Controls

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization. In this section, describe the technical control measures (**in place** or **planned**) that are intended to meet the protection requirements of the major application.

## 6.MA.1 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. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users.

### 6.MA.1.1 Identification

Identification is the means by which a user *provides* a claimed identity to the system. The most common form of identification is the user ID. In this section of the plan, briefly describe how the major application identifies access to the system

Unique Identification**.** An organization should require users to identify themselves uniquely before being allowed to perform any actions on the system unless user anonymity or other factors dictate otherwise.

Correlate Actions to Users. The system should internally maintain the identity of all active users and be able to link actions to specific users. (See Section 6.MA.4, Audit Trails.)

Maintenance of User IDs. An organization should ensure that all user IDs belong to currently authorized users. Identification data must be kept current by adding new users and deleting former users.

Inactive User IDs. User IDs that are inactive on the system for a specific period of time (e.g., three months) should be disabled.

### 6.MA.1.2 Authentication

Authentication is the means of establishing the *validity* of a user's claimed identity to the system. There are three means of authenticating a user's identity *which can be used alone or in combination*: something the individual *knows* (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key); something the individual *possesses* (a token -- e.g., an ATM card or a smart card); and something the individual *is* (a biometrics -- e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint).

In this section, describe the major application's authentication control mechanisms. Below is a list of items that should be considered in the description:

- Describe the method of user authentication (password, token, and biometrics).

- If a password system is used, provide the following specific information:

  - Allowable character set,
  - Password length (minimum, maximum),
  - Password aging time frames and enforcement approach,
  - Number of generations of expired passwords disallowed for use,
  - Procedures for password changes,
  - Procedures for handling lost passwords, and
  - Procedures for handling password compromise.

- Procedures for training users and the materials covered.

**Note:** The recommended minimum number of characters in a password is six to eight characters in a combination of alpha, numeric, or special characters.

- Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).

- Describe any biometrics controls used. Include a description of how the biometrics controls are implemented on the system.

- Describe any token controls used on the system and how they are implemented.

  - Are special hardware readers required?

  - Are users required to use a unique Personal Identification Number (PIN)?

  - Who selects the PIN, the user or System Administrator?

  - Does the token use a password generator to create a one-time password?

- Is a challenge-response protocol used to create a one-time password?

- Describe the level of enforcement of the access control mechanism (network, operating system, and application).

- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).

- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are transmitted and stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords, passwords are encrypted while in transmission).

- State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.

- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.

- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are allowed only for batch applications).

- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.

- If digital signatures are used, the technology must conform with Federal Information Processing Standards (FIPS) 186, *Digital Signature Standard* and FIPS 180-1, *Secure Hash Standard* issued by NIST, unless a waiver has been granted. Describe any use of digital or electronic signatures. Address the following specific issues:

    - State the digital signature standards used. If the standards used are not NIST standards, please state the date the waiver was granted and the name and title of the official granting the waiver.

    - Describe the use of electronic signatures and the security control provided.

    - Discuss cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction and archiving.

## 6.MA.2 Logical Access Controls (Authorization/Access Controls)

Logical access controls are the system-based mechanisms used to specify who or what (e.g., in the case of a process) is to have access to a specific system resource and the type of access that is permitted.

In this section, discuss the controls in place to authorize or restrict the activities of users and system personnel within the application. Describe hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists). The following are areas that should be considered.

- Describe formal policies that define the authority that will be granted to each user or class of users. Indicate if these policies follow the concept of least privilege which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more. Include in the description the procedures for granting new users access and the procedures for when the role or job function changes.

- Identify whether the policies include separation of duties enforcement to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion.

- Describe the application's capability to establish an Access Control List or register of the users and the types of access they are permitted.

- Indicate whether a manual Access Control List is maintained.

- Indicate if the security software allows application owners to restrict the access rights of other application users, the general support system administrator, or operators to the application programs, data, or files.

- Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.

- Indicate how often Access Control Lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application.

- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users.

- Describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users. This "discretionary access control" may be appropriate for some applications, and inappropriate for others. Document any evaluation made to justify/support use of "discretionary access control."

- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.

- Describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends. Discuss in-place restrictions.

- Indicate if encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. (If encryption is used primarily for authentication, include this information in the section above.) If encryption is used as part of the access controls, provide information about the following:

  - What cryptographic methodology (e.g., secret key and public key) is used? If a specific off-the-shelf product is used, provide the name of the product. If the product and the implementation method meet federal standards (e.g., Data Encryption Standard, Digital Signature Standard), include that information.

  - Discuss cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving.

- If your application is running on a system that is connected to the Internet or other wide area network(s), discuss what additional hardware or technical controls have been installed and implemented to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities.

- Describe any type of secure gateway or firewall in use, including its configuration, (e.g., configured to restrict access to critical system resources and to disallow certain types of traffic to pass through to the system).

- Provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices, and if additional passwords or tokens are required.

- Identify whether internal security labels are used to control access to specific information types or files, and if such labels specify protective measures or indicate additional handling instructions.

- Indicate if host-based authentication is used. (This is an access control approach that grants access based on the identity of the host originating the request, instead of the individual user requesting access.)

It is recommended that a standardized log-on banner be placed on the system. Public Law 99-474 requires that a warning message be displayed, notifying unauthorized users that they have accessed a U.S. Government computer system and unauthorized use can be punished by fines or imprisonment. Some of the systems now in use are intended for unrestricted use by the general public (e.g., Internet-based systems used for widespread public information dissemination), a situation not prevalent when Public Law 99-474 was enacted. Due to their adverse impact on the intended user population, highly restrictive warning banners may not be appropriate. The choice of which screen warning banner to implement is up to the system owner and should be based on system-specific technology limitations, data sensitivity, or other unique system requirements. In this section, describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Department of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

| Example Warning Banners | | |
|---|---|---|
| Banner | Selection Rationale | Approved by DOJ |
| **WARNING**WARNING**WARNING**<br>This is a (Agency) computer system. (Agency) computer systems are provided for the processing of Official U.S. Government information only. All data contained on (Agency) computer systems is owned by the (Agency) *may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner,* by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crime found on (Agency) computer systems. *USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING and DISCLOSURE.*<br>**WARNING**WARNING**WARNING** | System is for Government use only and all transmissions may be monitored. | Yes |
| **WARNING**WARNING**WARNING**<br>This is a United States (Agency) computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.<br><br>All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized, constitutes consent to these terms.<br>**WARNING**WARNING**WARNING** | System is for Government use only. Monitoring is only performed in support of system operations and to investigate potential security events. | Yes |
| The seals, initials, and agency identification can not be used without the written permission of the agency. | Information dissemination. System open to the general public. Associated risks are denial of access and transitory embarrassment to the agency. | No |
| None | Information dissemination. System open to the general public. Associated risks are denial of access and transitory embarrassment to the agency. | No |

## 6.MA.3 Public Access Controls

Where an organization's application promotes or permits public access, additional security controls are needed to protect the integrity of the application and the confidence of the public in the application. Such controls include segregating information made directly accessible to the public from official organization records.

Public access systems are subject to a greater threat from outside attacks. In public access systems, users are often anonymous and untrained in the system and their responsibilities. Attacks on public access systems could have a substantial impact on the organization's reputation and the level of public trust and confidence. Threats from insiders are also greater (e.g., errors introduced by disgruntled employees or unintentional errors by untrained users).

If the public accesses the major application, describe the additional controls in place. The following list describes the type of controls that might provide protection in a public access system and issues that should be considered. It is not intended to include all possible controls or issues.

- Some form of identification and authentication (this may be difficult).
- Access control to limit what the user can read, write, modify, or delete.
- Controls to prevent public users from modifying information on the system.
- Digital signatures.
- CD-ROM for on-line storage of information for distribution.
- Put copies of information for public access on a separate system.
- Prohibit public to access "live" databases.
- Verify that programs and information distributed to the public are virus-free.
- Audit trails and user confidentiality.
- System and data availability.
- Legal considerations.

## 6.MA.4 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 a means to help accomplish *several* security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. In this section, describe the audit trail mechanisms in place. A list of items to consider are provided below:

- Does the audit trail support accountability by providing a trace of user actions?
- Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased?
- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection?
- Are audit trails used as online tools to help identify problems other than intrusions as they occur?
- Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them? In general, an event record should specify:
  - Type of event;
  - When the event occurred;
  - User ID associated with the event; and
  - Program or command used to initiate the event.
- Is access to online audit logs strictly controlled?
- Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?
- Is the confidentiality of audit trail information protected if, for example, it records personal information about users?
- Describe how frequently audit trails are reviewed and whether there are review guidelines.
- Can the audit trail be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information?

- Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem?

- Audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, can be used in a real-time or near real-time fashion. Does the organization use the many types of tools that have been developed to help reduce the amount of information contained in audit records, as well as to distill useful information from the raw data?

Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. The Department of Justice has advised that an ambiguity in U.S. law makes it unclear whether keystroke monitoring is considered equivalent to an unauthorized telephone wiretap. If keystroke monitoring is used in audit trails, organizations should have a written policy and notify users. The Rules of Behavior may be one vehicle for distributing the information. If keystroke monitoring is used, provide reference to the policy and the means of notification. Also indicate whether the Department of Justice has reviewed the policy.

## 5.GSS General Support System – Operational Controls

The operational controls address security mechanisms that focus on methods that primarily are 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. In this section, describe the operational control measures (**in place** or **planned**) that are intended to meet the protection requirements of the general support system.

### 5.GSS.1 Personnel Controls

The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. All too often, systems experience disruption, damage, loss, or other adverse impact due to the well-intentioned actions of individuals authorized to use or maintain a system (e.g., the programmer who inserts one minor change, then installs the program into the production environment without testing).

In this section, include detailed information about the following personnel security measures. It is recommended that most of these measures be included as part of the rules of behavior. If they are incorporated in the rules of behavior, reference the applicable section.

- Have all positions been reviewed for sensitivity level? If all positions have not been reviewed, state the planned date for completion of position sensitivity analysis.

- A statement as to whether individuals have received the background screening appropriate for the position to which they are assigned. If all individuals have not had appropriate background screening, include the date by which such screening will be completed.

- If individuals are permitted system access prior to completion of appropriate background screening, describe the conditions under which this is allowed and any compensating controls to mitigate the associated risk.

- Are users access restricted (least privilege) to data files, to processing capability, or to peripherals and type of access (e.g., read, write, execute, delete) to the minimum necessary to perform the job?

- Are critical functions divided among different individuals (separation of duties) to ensure that no individual has all necessary authority or information access which could result in fraudulent activity?

- Is there a process for requesting, establishing, issuing, and closing user accounts?

- What mechanisms are in place for holding user's responsible for their actions?

- What are the termination procedures for a friendly termination and an unfriendly termination?

## 5.GSS.2 Physical and Environmental Protection

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical and environmental security program should address the following seven topics which are explained below. In this section, briefly describe the physical and environmental controls in place or planned for the general support system.

### 5.GSS.2.1 Explanation of Physical and Environment Security

Access Controls. Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a local area network (LAN) server. Physical access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation. It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied.

Fire Safety Factors. Building fires are a particularly important security threat because of the potential for complete destruction of both hardware and data, the risk to human life, and the pervasiveness of the damage. Smoke, corrosive gases, and high humidity from a localized fire can damage systems throughout an entire building. Consequently, it is important to evaluate the fire safety of buildings that house systems.

Failure of Supporting Utilities. Systems and the people who operate them need to have a reasonably well-controlled operating environment. Consequently, failures of electric power, heating and air-conditioning systems, water, sewage, and other utilities will usually cause a service interruption and may damage hardware. Organizations should ensure that these utilities, including their many elements, function properly.

Structural Collapse. Organizations should be aware that a building may be subjected to a load greater than it can support. Most commonly this is a result of an earthquake, a snow load on the roof beyond design criteria, an explosion that displaces or cuts structural members, or a fire that weakens structural members.

Plumbing Leaks. While plumbing leaks do not occur every day, they can be seriously disruptive. An organization should know the location of plumbing lines that might endanger system hardware and take steps to reduce risk (e.g., moving hardware, relocating plumbing lines, and identifying shutoff valves.)

Interception of Data. Depending on the type of data a system processes, there may be a significant risk if the data is intercepted. Organizations should be aware that there are three routes of data interception: direct observation, interception of data transmission, and electromagnetic interception.

Mobile and Portable Systems. The analysis and management of risk usually has to be modified if a system is installed in a vehicle or is portable, such as a laptop computer. The system in a vehicle will share the risks of the vehicle, including accidents and theft, as well as regional and local risks. Organizations should:

- Securely store laptop computers when they are not in use.

- Encrypt data files on stored media, when cost-effective, as a precaution against disclosure of information if a laptop computer is lost or stolen.

### 5.GSS.2.2 Computer Room Example

Appropriate and adequate controls will vary depending on the individual system requirements. The example list shows the types of controls for an application residing on a system in a computer room. The list is not intended to be all inclusive or to imply that all systems should have all controls listed.

**Example Physical/Environmental Controls For Computer Room**

**In Place**
Card keys for building and work-area entrances
Twenty-four hour guards at all entrances/exits
Cipher lock on computer room door
Raised floor in computer room
Dedicated cooling system
Humidifier in tape library
Emergency lighting in computer room
Four fire extinguishers rated for electrical fires
One B/C rated fire extinguisher
Smoke, water, and heat detectors
Emergency power-off switch by exit door
Surge suppressor
Emergency replacement server
Zoned dry pipe sprinkler system
Uninterruptable power supply for LAN servers
Power strips/suppressors for peripherals
Power strips/suppressors for computers
Controlled access to file server room

**Planned**
Plastic sheets for water protection, August 1999
Closed-circuit television monitors, January 2000

## 5.GSS.3 Production, Input/Output Controls

In this section, provide a synopsis of the procedures in place that support the general support system. Below is a sampling of topics that should be reported.

- User support.

- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.
- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media.
- Audit trails for receipt of sensitive inputs/outputs.
- Procedures for restricting access to output products.
- Procedures and controls used for transporting or mailing media or printed output.
- Internal/external labeling for appropriate sensitivity (e.g., Privacy Act, Proprietary).
- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates).
- Audit trails for inventory management.
- Media storage vault or library physical and environmental protection controls and procedures.
- Procedures for sanitizing electronic media for reuse (e.g., overwrite or degaussing of electronic media).
- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse.
- Procedures for shredding or other destructive measures for hardcopy media when no longer required.

## 5.GSS.4 Contingency Planning (Continuity of Support)

General support systems require appropriate emergency, backup, and contingency plans. These plans should be tested regularly to assure the continuity of support in the event of system failure. Also, these plans should be known to users and coordinated with their plans for applications.

Describe the procedures (contingency plan) that would be followed to ensure the system continues to process all critical applications if a disaster should occur and provide a reference to the detailed plans. Include consideration of the following questions in this description:

- Is tested contingency plan in place to permit continuity of mission-critical functions in the event of a catastrophic event?

- Is tested disaster recovery plan in place for all supporting IT systems and networks?

- Is formal written emergency operating procedure posted or located to facilitate their use in emergency situations?

- How often are contingency, disaster, and emergency plans tested?

- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

Include descriptions of the following controls.

- Any agreements for backup processing (e.g., hotsite contract with a commercial service provider).

- Documented backup procedures including frequency (daily, weekly, monthly) and scope (full backup, incremental backup, and differential backup).

- Location of stored backups (off-site or on-site).

- Generations of backups kept.

- Coverage of backup procedures, e.g., what is being backed up.

## 5.GSS.5 Hardware and System Software Maintenance Controls

These controls are used to monitor the installation of, and updates to, hardware, operating system software, and other software to ensure that the hardware and software function as expected, and that a historical record is maintained of application changes. These controls may also be used to ensure that only authorized software is installed on the system. Such controls may include a hardware and software configuration policy that grants managerial approval (re-authorize processing) to modifications and requires that changes be documented. Other controls include products and procedures used in auditing for, or preventing, illegal use of shareware or copyrighted software. In this section, provide several paragraphs on the hardware and system software maintenance controls in place or planned. The following statements are examples of items that should be addressed in responding to this section:

- Are procedures in place to ensure that maintenance and repair activities are accomplished without adversely affecting system security? Consider the following items:

- Restriction/controls on those who perform maintenance and repair activities.
- Special procedures for performance of emergency repair and maintenance.
- Management of hardware/software warranties and upgrade policies to maximize use of such items to minimize costs.
- Procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site).
- Procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements.

Describe the configuration management procedures for the system. Consider the following items in the description:

- Version control that allows association of system components to the appropriate system version.
- Procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production.
- Impact analyses to determine the effect of proposed changes on existing security controls to include the required training for both technical and user communities associated with the change in hardware/software.
- Change identification, approval, and documentation procedures.
- Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes.
- Are test data "live" data or made-up data?
- How are emergency fixes handled?

Describe the policies for handling copyrighted software or shareware. Consider including in this description answers to the following questions:

- Are there organizational policies against illegal use of copyrighted software or shareware?
- Do the policies contain provisions for individual and management responsibilities and accountability, including penalties?

- Are periodic audits conducted of users' computers (PCs) to ensure only legal licensed copies of software are installed?

- What products and procedures are used to protect against illegal use of software?

- Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?

## 5.GSS.6 Integrity Controls

Integrity controls are used to protect the operating system, applications, and information in the system from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered.

In this section, describe any controls that provide assurance to users that the information has not been altered and that the system functions as expected. The following questions are examples of some of the controls that fit in this category:

- Is virus detection and elimination software installed? If so, are there procedures for:

  - Updating virus signature files;

  - Automatic and/or manual virus scans (automatic scan on network log-in, automatic scan on client/server power on, automatic scan on diskette insertion, automatic scan on download from an unprotected source such as the Internet, scan for macro viruses); and

  - Virus eradication and reporting?

- Are reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.

- Are password crackers/checkers used?

- Are
- integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? Techniques include consistency and reasonableness checks and validation during data entry and processing. Describe the integrity controls used within the system.

- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?

- Is message authentication used in the application to ensure that the sender of a message is known and that the message has not been altered during transmission? State whether message authentication has been determined to be appropriate for your system. If so, describe the methodology.

## 5.GSS.7 Documentation

Documentation is a security control in that it explains how software/hardware is to be used and formalizes security and operational procedures specific to the system. Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security on the support system, including backup and contingency activities, as well as descriptions of user and operator procedures.

List the documentation maintained for the general support system. An example list is provided to show the type of documentation that would normally be maintained for a system. The list is not intended to be all-inclusive or imply that all systems should have all items listed.

**Examples of General Support System Documentation**

- Vendor-supplied documentation of hardware
- Vendor-supplied documentation of software
- General support system security plan
- Testing procedures and results
- Standard operating procedures
- Emergency procedures
- Contingency plans
- Disaster recovery plans
- User rules of behavior
- User manuals
- Risk assessment
- Backup procedures
- Authorize processing documents and statements

## 5.GSS.8 Security Awareness and Training

The Computer Security Act requires federal agencies to provide mandatory periodic training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of the federal agency. This includes

contractors as well as employees of the agency. OMB Circular A-130, Appendix III, issued in 1996, enforces such mandatory training by requiring its completion prior to granting access to the system and through periodic refresher training for continued access. Therefore, each user must be versed in acceptable rules of behavior for the system before being allowed access to the system. The training program should also inform the user on how to get help when having difficulty using the system and procedures for reporting security incidents.

Access provided to members of the public should be constrained by controls in the applications, and training should be within the context of those controls and may consist only of notification at the time of access.

Include in this section of the plan information about the following:

- The awareness program for the system (posters, booklets, and trinkets).
- The type and frequency of system-specific training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the-job training).
- The procedures for assuring that employees and contractor personnel have been provided adequate training.

**Note:** Contractor employees are required to receive the same level of automated information systems security awareness and training as federal employees. This training requirement should be included as appropriate in all contracts.

## 5.GSS.9 Incident Response Capability

A computer security incident is an adverse event in a computer system or network caused by a failure of a security mechanism or an attempted or threatened breach of these mechanisms[3]. Computer security incidents are becoming more common and their impact far-reaching. When faced with an incident, an organization should be able to respond quickly in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident. OMB Circular A-130 requires each agency to ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. In this section, describe the incident handling procedures in place for the general support system. Areas of consideration include:

[3] Schultz, Brown, Longstaff. Responding to Computer Security Incidents: Guidelines for Incident Handling, U.C. Technical Report UCRL-104689, 1990.

- Is there a formal incident response capability (in-house or external) available? If there is no capability established, is there a help desk or similar organization available for assistance?
  - Are there procedures for reporting incidents handled either by system personnel or externally?
  - Are there procedures for recognizing and handling incidents, i.e., what files and logs should be kept, who to contact, and when?
- Who receives and responds to alerts/advisories, e.g., vendor patches, exploited vulnerabilities?
- What preventative measures are in place?
  - Intrusion detection tools
  - Automated audit logs
  - Penetration testing

# 6.GSS General Support System - Technical Controls

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations – and should be consistent with the management of security within the organization. In this section, describe the technical control measures (**in place** or **planned**) that are intended to meet the protection requirements of the general support system.

## 6.GSS.1 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. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users.

### 6.GSS.1.1 Identification

Identification is the means by which a user *provides* a claimed identity to the system. The most common form of identification is the user ID. In this section of the plan, describe how the general support system identifies access to the system.

Unique Identification**.** An organization should require users to identify themselves uniquely before being allowed to perform any actions on the system unless user anonymity or other factors dictate otherwise.

Correlate Actions to Users. The system should internally maintain the identity of all active users and be able to link actions to specific users. (See Section 6.GSS.4, Audit Trails.)

Maintenance of User IDs. An organization should ensure that all user IDs belong to currently authorized users. Identification data must be kept current by adding new users and deleting former users.

Inactive User IDs. User IDs that are inactive on the system for a specific period of time (e.g., three months) should be disabled.

### 6.GSS.1.2 Authentication

Authentication is the means of establishing the *validity* of a user's claimed identity to the system. There are three means of authenticating a user's identity *which can be used alone or in combination*: something the individual *knows* (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key); something the individual *possesses* (a token -- e.g., an ATM card or a smart card); and something the individual *is* (a biometrics -- e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint).

In this section, describe the general support system's authentication control mechanisms. Below is a list of items that should be considered in the description:

- Describe the method of user authentication (password, token, and biometrics).
- If a password system is used, provide the following specific information:
  - Allowable character set;
  - Password length (minimum, maximum);
  - Password aging time frames and enforcement approach;
  - Number of generations of expired passwords disallowed for use;
  - Procedures for password changes;
  - Procedures for handling lost passwords, and
  - Procedures for handling password compromise.
- Procedures for training users and the materials covered.

**Note:** The recommended minimum number of characters for a password is six to eight characters in a combination of alpha, numeric, or special characters.

- Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).
- Describe any biometrics controls used. Include a description of how the biometrics controls are implemented on the system.
- Describe any token controls used on this system and how they are implemented.
  - Are special hardware readers required?

  - Are users required to use a unique Personal Identification Number (PIN)?
  - Who selects the PIN, the user or System Administrator?
  - Does the token use a password generator to create a one-time password? and
  - Is a challenge-response protocol used to create a one-time password?

- Describe the level of enforcement of the access control mechanism (network, operating system, and application).
- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).
- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are transmitted and stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords).
- State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.
- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.
- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).
- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.
- If digital signatures are used, the technology must conforms with FIPS 186, *Digital Signature Standard* and FIPS 180-1, *Secure Hash Standard* issued by NIST, unless a waiver has been granted. Describe any use of digital or electronic signatures. Address the following specific issues:
  - State the digital signature standards used. If the standards used are not NIST standards, please state the date the waiver was granted, and the name and title of the official granting the waiver.

- Describe the use of electronic signatures and the security control provided.

- Discuss cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction and archiving.

## 6.GSS.2 Logical Access Controls (Authorization/Access Controls)

Logical access controls are the system-based mechanisms used to specify who or what (e.g., in the case of a process) is to have access to a specific system resource and the type of access that is permitted.

In this section, discuss the controls in place to authorize or restrict the activities of users and system personnel within the general support system. Describe hardware or software features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists). The following are areas that should be considered.

- Describe formal policies that define the authority that will be granted to each user or class of users. Indicate if these policies follow the concept of least privilege which requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more. Include in the description the procedures for granting new users access and the procedures for when the role or job function changes.

- Identify whether the policies include separation of duties enforcement to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion.

- Describe the system's capability to establish an Access Control List or register of the users, and the types of access they are permitted.

- Indicate whether a manual Access Control List is maintained.

- Indicate if the security software allows application owners to restrict the access rights of other application users, the general support system administrator, or operators to the application programs, data, or files.

- Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.

- Indicate how often Access Control Lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application.

- Describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users. This "discretionary access control" may be appropriate for some applications, and inappropriate for others. Document any evaluation made to justify/support use of "discretionary access control."

- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users.

- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.

- Describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends. Discuss in-place restrictions.

- Indicate if encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. (If encryption is used primarily for authentication, include this information in the section above.) If encryption is used as part of the access controls, provide information about the following:

  - What cryptographic methodology (e.g., secret key and public key) is used? If a specific off-the-shelf product is used, provide the name of the product. If the product and the implementation method meets federal standards (e.g., Data Encryption Standard, Digital Signature Standard), include that information.

  - Discuss cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving.

- If the general support system is connected to the Internet or other wide area network(s), discuss what additional hardware or technical controls have been installed and implemented to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities.

- Describe any type of secure gateway or firewall in use, including its configuration, (e.g., configured to restrict access to critical system resources and to disallow certain types of traffic to pass through to the system).

- Provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices and if additional passwords or tokens are required.

- Identify whether internal security labels are used to control access to specific information types or files, and if such labels specify protective measures or indicate additional handling instructions.

- Indicate if host-based authentication is used. (This is an access control approach that grants access based on the identity of the host originating the request, instead of the individual user requesting access.)

In addition, documentation for a system should include a standardized log-on banner. Public Law 99-474 requires that a warning message be displayed, notifying unauthorized users that they have accessed a U.S. Government computer system and unauthorized use can be punished by fines or imprisonment. Some of the systems now in use are intended for unrestricted use by the general public (e.g., Internet-based systems used for widespread public information dissemination), a situation not prevalent when Public Law 99-474 was enacted. Thus, due to their adverse impact on the intended user population, highly restrictive warning banners may not be appropriate. The choice of which screen warning banner to implement is up to the system owner and should be based on system-specific technology limitations, data sensitivity, or other unique system requirements. In this section, describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Department of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

| Example Warning Banners | | |
|---|---|---|
| Banner | Selection Rationale | Approved by DOJ |
| **WARNING**WARNING**WARNING**<br>This is a (Agency) computer system. (Agency) computer systems are provided for the processing of Official U.S. Government information only. All data contained on (Agency) computer systems is owned by the (Agency) *may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner,* by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crime found on (Agency) computer systems. *USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING and DISCLOSURE.*<br>**WARNING**WARNING**WARNING** | System is for Government use only and all transmissions may be monitored. | Yes |
| **WARNING**WARNING**WARNING**<br>This is a United States (Agency) computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.<br><br>All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized, constitutes consent to these terms.<br>**WARNING**WARNING**WARNING** | System is for Government use only. Monitoring is only performed in support of system operations and to investigate potential security events. | Yes |
| The seals, initials, and agency identification can not be used without the written permission of the agency. | Information dissemination. System open to the general public. Associated risks are denial of access and transitory embarrassment to the agency. | No |
| None | Information dissemination. System open to the general public. Associated risks are denial of access and transitory embarrassment to the agency. | No |

## 6.GSS.3 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 a means to help accomplish *several* security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. In this section, describe the audit trail mechanisms in place. A list of items to consider are provided below:

- Does the audit trail provide accountability by providing a trace of user actions?
- Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased?
- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection?
- Are audit trails used as online tools to help identify problems other than intrusions as they occur?
- Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them. In general, an event record should specify:
  - Type of event;
  - When the event occurred;
  - User ID associated with the event; and
  - Program or command used to initiate the event.
- Is access to online audit logs strictly controlled?
- Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?
- Is the confidentiality of audit trail information protected if, for example, it records personal information about users?
- Describe how frequently audit trails are reviewed and whether there are review guidelines.
- Can the audit trail be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.

- Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem?

- Audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, can be used in a real-time, or near real-time, fashion. Does the organization use the many types of tools that have been developed to help reduce the amount of information contained in audit records, as well as to distill useful information from the raw data?

Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. The Department of Justice has advised that an ambiguity in U.S. law makes it unclear whether keystroke monitoring is considered equivalent to an unauthorized telephone wiretap. If keystroke monitoring is used in audit trails, organizations should have a written policy and notify users. The Rules of Behavior may be one vehicle for distributing the information. If keystroke monitoring is used, provide reference to the policy and the means of notification. Also indicate whether the Department of Justice has reviewed the policy.

# Rules of Behavior

HYPOTHETICAL GOVERNMENT AGENCY'S (HGA)
FINANCIAL INFORMATION SYSTEM

## 1. Introduction

The following rules of behavior are to be followed by all users of the HGA's Financial Information System (HFIS). The rules clearly delineate responsibilities of and expectations for all individuals with access to the HFIS. Non-compliance of these rules will be enforced through sanctions commensurate with the level of infraction. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

## 1. Responsibilities

The Chief, Financial Information Systems Branch, is responsible for ensuring an adequate level of protection is afforded to the FIS, through an appropriate mix of technical, administrative, and managerial controls. The Branch Chief develops policies and procedures, ensures the development and presentation of user and contractor awareness sessions, and inspects and spot checks to determine that an adequate level of compliance with security requirements exists. The Branch Chief is responsible for periodically conducting vulnerability analyses to help determine if security controls are adequate. Special attention will be given to those new and developing technologies, systems, and applications that can open or have opened vulnerabilities in HGA's security posture.

## 2. Other Policies and Procedures

The rules are not to be used in place of existing policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing HFIS. The rules are consistent with the policy and procedures described in the following directives:

HGA IRM Computer Security Handbook. The newly revised Handbook, dated April 4, 1998, contains computer security guidance on a wide range of topics, i.e., personnel security, incident handling, access control mechanisms. This document contains responsibilities for the SECURITY OFFICE, HGA managers, and users.

HFIS Access Control Management Directive. This directive, dated May 6, 1997, contains responsibilities for HFIS data owners and application administrators.

Draft HFIS Access Control Management Directive. The draft HFIS Access Control Management Directive contains specific responsibilities for the security officer.

Letter for External (non-HGA) Users. A letter for Non-HGA users which transmits the applicable HGA policies should be provided to all non-HGA users while using HFIS, or when using HGA systems and applications in general. These responsibilities should be included in training HGA provides for agency security points of contact, and should be included in interagency agreements or other formal agreements or documents between HGA and other organizations.

3. Application Rules

4.1 Work at home. HGA Personnel Policy Directive 97-03, dated March 10, 1997, authorizes Division Directors to designate specific employees (e.g., critical job series, employees on maternity leave, employees with certain medical conditions) as eligible for working at home. Any work-at-home arrangement should:

- be in writing;
- identify the time period the work at home will be allowed;
- identify what government equipment and supplies will be needed by the employee at home, and how that equipment and supplies will be transferred and accounted for;
- identify if telecommuting will be needed and allowed (this issue should be discussed between the requesting organization, Information Resources Management Division (IRMD), and the SECURITY OFFICE; see Section 4.2); and
- be reviewed by HGA's personnel office prior to commencement.

4.2 Dial-in access. The IRM Division Director may authorize dial-in access to HFIS. It is understood that dial-in access poses additional security risks, but may become necessary for certain job functions. If dial-in access is allowed, IRMD and the security office will regularly review telecommunications logs and HGA phone records, and conduct spot-checks to determine if HGA business functions are complying with controls placed on the use of dial-in lines. All dial-in calls will use one-time passwords. If dial-in access is allowed to other applications on the system on which HFIS resides, the managers of those applications should also determine if such access could pose a risk to HFIS data.

4.3 Connection to the Internet. Some HGA personnel have access to the Internet. HGA should ensure that the user authentication required for access is adequate to protect HFIS programs and data. If such access is allowed, HGA should carefully document all external connections to ensure access to HFIS is limited to controlled points of entry.

4.4 Protection of software copyright licenses. All copyright licenses associated with the COTS HFIS software are complied with by HGA personnel, as well as by contractors responsible for developing and maintaining HFIS. HGA requires that all copyright licenses for all PC-based and LAN-based software used by HFIS program personnel and contractor personnel are understood and that these personnel comply with the license requirements. End users, supervisors, and function managers are ultimately responsible for this compliance.

4.5 Unofficial use of government equipment. Users should be aware that personal use of information resources is not authorized.

I acknowledge receipt of, understand my responsibilities, and will comply with the rules of behavior for the HFIS.

_____ _____

Signature of User Date

# Rules of Behavior

## Hypothetical Government Agency's (HGA) Backbone Local Area Network

The rules of behavior contained in this document are to be followed by all users of the HGA Local Area Network (LAN). Users will be held accountable for their actions on the LAN. If an employee violates HGA policy regarding the rules of the LAN, they may be subject to disciplinary action at the discretion of HGA management. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

Work at home. HGA Personnel Policy Directive 97-03, dated March 10, 1997, authorizes Division Directors to designate specific employees (e.g., critical job series, employees on maternity leave, employees with certain medical conditions) as eligible for working at home. Any work at home arrangement should:

- be in writing;
- identify the time period the work at home will be allowed;
- identify what government equipment and supplies will be needed by the employee at home, and how that equipment and supplies will be transferred and accounted for;
- identify if telecommuting will be needed and allowed (this issue should be discussed between the requesting organization, Information Resources Management Division (IRMD), and the SECURITY OFFICE; see Dial-in access section below); and
- be reviewed by HGA's personnel office prior to commencement.

Dial-in access. No dial-in access is used to access LAN servers. However, if a justifiable need occurs, the IRM Division Director may authorize dial-in access to a LAN server. It is understood that dial-in access would pose additional security risks, but may become necessary for certain job functions. If dial-in access is allowed, IRMD and the SECURITY OFFICE will regularly review telecommunications logs and HGA phone records, and conduct spot-checks to determine if HGA business functions are complying with controls placed on the use of dial-in lines. All dial-in calls will use one-time passwords.

Connection to the Internet. Some HGA personnel have access to the Internet. Access to the Internet should be closely controlled by the SECURITY OFFICE. HGA divisions, staff managers, and technicians should know that only HGA-authorized Internet

connections will be allowed, and that all connections must conform to HGA's security and communications architecture.

Protection of copyright licenses (software) – LAN and PC users are not to download LAN-resident software. Audit logs will be reviewed to determine whether employees attempt to access LAN servers on which valuable, off-the-shelf software resides, but to which users have not been granted access. Audit logs will also show users' use of a "copy" command; this may indicate attempts to illegally download software. Unauthorized copying of PC-based software is also prohibited.

Unofficial use of government equipment – Users should be aware that personal use of information resources – LAN and PC – is not authorized.

Use of passwords – Users are to use passwords of a length specified by the LAN system administrators – a mix of six (6) alpha and numeric characters, they are to keep passwords confidential and are not to share passwords with anyone.

System privileges – Users are given access to the LAN based on a need to perform specific work. Users are to work within the confines of the access allowed and are not to attempt access to systems or applications to which access has not been authorized.

Individual accountability – Users will be held accountable for their actions on the LAN. This is stressed during computer security awareness training sessions

Restoration of service – The availability of the LAN is a concern to all users. All users are responsible for ensuring the restoration of services in the event the LAN is unoperational.

I acknowledge receipt of, understand my responsibilities, and will comply with the rules of behavior for the HGA Backbone LAN.

_____ _____

Signature of User Date

# Template for Security Plan

## Major Application Security Plan

### SYSTEM IDENTIFICATION

Date:

**System Name/Title**
- Unique Identifier & Name Given to the System

**Responsible Organization**
- List organization responsible for the application

**Information Contact(s)**
- Name of person(s) knowledgeable about, or the owner of, the system.

Name
Title
Address
Phone

**Assignment of Security Responsibility**
- Name of person responsible for security of the system.

Name
Title
Address
Phone

**System Operational Status**

If more than one status is selected, list which part of the system is covered under each status.

- Operational
- Under Development
- Undergoing a major modification

**General Description/Purpose**
- Describe the function or purpose of the application and the information processed.
- Describe the processing flow of the application from system input to system output.
- List user organizations (internal & external) and type of data and processing provided.

**System Environment**

- Provide a general description of the technical system. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.)
- Describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources.
- Include any security software protecting the system and information.

**System Interconnection/Information Sharing**

- List interconnected systems and system identifiers (if appropriate).
- If connected to an external system not covered by a security plan, provide a short discussion of any security concerns that need to be considered for protection.
- It is required that written authorization (MOUs, MOAs) be obtained prior to connection with other systems and/or sharing sensitive data/information. It should detail the rules of behavior that must be maintained by the interconnecting systems. A description of these rules must be included with the security plan or discussed in this section.

**Applicable Laws or Regulations Affecting the System**

- List any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.

**General Description of Information Sensitivity**

- Describe, in general terms, the information handled by the system and the need for protective measures. Relate the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability). For each of the three categories, indicate if the requirement is: **High, Medium, or Low**.
- Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.

## MANAGEMENT CONTROLS

**Risk Assessment and Management**

- Describe the risk assessment methodology used to identify the threats and vulnerabilities of the system. Include the date the review was conducted. If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.

**Review of Security Controls**

- List any independent security reviews conducted on the system in the last three years.

- Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

**Rules of Behavior**

- A set of rules of behavior in writing must be established for each system. The rules of behavior should be made available to every user prior to receiving access to the system. It is recommended that the rules contain a signature page to acknowledge receipt.
- The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. They should state the consequences of inconsistent behavior or non-compliance. They should also include appropriate limits on interconnections to other systems.
- Attach the rules of behavior for the system as an appendix and reference the appendix number in this section or insert the rules into this section.

**Planning for Security in the Life Cycle**

Determine which phase(s) of the life cycle the system, or parts of the system are in. Describe how security has been handled in the life cycle phase(s) the system is currently in.

**Initiation Phase**

- Reference the sensitivity assessment which is described in Section 3.7, Sensitivity of Information Handled.

**Development/Acquisition Phase**

- During the system design, were security requirements identified?
- Were the appropriate security controls with associated evaluation and test procedures developed before the procurement action?
- Did the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?
- Did the requirements permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented?
- If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security requirements identified and included in the acquisition specifications?

**Implementation Phase**

- Were design reviews and systems tests run prior to placing the system in production? Were the tests documented? Has the system been certified?
- Have security controls been added since development?
- Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?
- Include the date of the certification and accreditation. If the system is not authorized yet, include date when accreditation request will be made.

**Operation/Maintenance Phase**

- The security plan documents the security activities required in this phase.

**Disposal Phase**

- Describe in this section how information is moved to another system, archived, discarded, or destroyed. Discuss controls used to ensure the confidentiality of the information.
- Is sensitive data encrypted?
- How is information cleared and purged from the system?
- Is information or media purged, overwritten, degaussed or destroyed?

**Authorize Processing**

- Provide the date of authorization, name, and title of management official authorizing processing in the system.
- If not authorized, provide the name and title of manager requesting approval to operate and date of request.

## OPERATIONAL CONTROLS

**Personnel Security**

- Have all positions been reviewed for sensitivity level?
- Have individuals received background screenings appropriate for the position to which they are assigned.
- Is user access restricted to the minimum necessary to perform the job?
- Is there a process for requesting, establishing, issuing, and closing user accounts?
- Are critical functions divided among different individuals (separation of duties)?
- What mechanisms are in place for holding users responsible for their actions?
- What are the friendly and unfriendly termination procedures?

**Physical and Environmental Protection**

- Discuss the physical protection in the area where application processing takes place (e.g., locks on terminals, physical barriers around the building and processing area, etc.)
- Factors to address include physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, mobile and portable systems.

**Production, Input/Output Controls**

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to, application software should be listed. In this section, provide a synopsis of the procedures in place that support the operations of the application. Below is a sampling of topics that should be reported in this section.

- User Support - Is there a help desk or group that offers advice and can respond to

security incidents in a timely manner? Are there procedures in place documenting how to recognize, handle, and report incidents and/or problems?
- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information
- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media
- Audit trails for receipt of sensitive inputs/outputs
- Procedures for restricting access to output products
- Procedures and controls used for transporting or mailing media or printed output
- Internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary)
- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)
- Audit trails for inventory management
- Media storage vault or library-physical, environmental protection controls/procedures
- Procedures for sanitizing electronic media for reuse (e.g., overwriting or degaussing)
- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse
- Procedures for shredding or other destructive measures for hardcopy media when no longer required

**Contingency Planning**

Briefly describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan can be attached as an appendix.

- Include descriptions for the following:
  - Any agreements of backup processing
  - Documented backup procedures including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup)
  - Location of stored backups and generations of backups
- Are tested contingency/disaster recovery plans in place? How often are they tested?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?
- Coverage of backup procedures, e.g., what is being backed up?

**Application Software Maintenance Controls**

- Was the application software developed in-house or under contract?
- Does the government own the software? Was it received from another agency?
- Is the application software a copyrighted commercial off-the-shelf product or shareware? Has it been properly licensed and enough copies purchased for all systems?

- Is there a formal change control process in place and if so, does it require that all changes to the application software be tested and approved before being put into production?
- Are test data "live" data or made-up data?
- Are all changes to the application software documented?
- Are test results documented?
- How are emergency fixes handled?
- Are there organizational policies against illegal use of copyrighted software, shareware?
- Are periodic audits conducted of users' computers to ensure only legal licensed copies of software are installed?
- What products and procedures are used to protect against illegal use of software?
- Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?

**Data Integrity/Validation Controls**

- Is virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?
- Is reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Is password crackers/checkers used?
- Is integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?
- Are intrusion detection tools installed on the system?
- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?
- Is penetration testing performed on the system? If so, what procedures are in place to ensure they are conducted appropriately?
- Is message authentication used in the application to ensure that the sender of a message is known and that the message has not been altered during transmission?

**Documentation**

Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security in the application and the support systems(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures.

- List the documentation maintained for the application (vendor documentation of hardware/software, functional requirements, security plan, general system security plan, application program manuals, test results documents, standard operating procedures, emergency procedures, contingency plans, user rules/procedures, risk assessment, certification/accreditation statements/documents, verification reviews/site inspections.)

### Security Awareness and Training

- Describe the awareness program for the application (posters, booklets, and trinkets).
- Describe the type and frequency of application-specific and general support system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the job training).
- Describe the procedures for assuring that employees and contractor personnel have been provided adequate training.

## TECHNICAL CONTROLS

### Identification and Authentication

- Describe the major application's authentication control mechanisms.
- Describe the method of user authentication (password, token, and biometrics)
- Provide the following if an additional password system is used in the application:
  - password length (minimum, maximum)
  - allowable character set,
  - password aging time frames and enforcement approach,
  - number of generations of expired passwords disallowed for use
  - procedures for password changes (after expiration and forgotten/lost)
  - procedures for handling password compromise
- Indicate the frequency of password changes, describe how changes are enforced, and identify who changes the passwords (the user, the system, or the system administrator).
- Describe how the access control mechanism support individual accountability and audit trails (e.g., passwords are associated with a user ID that is assigned to a single person).
- Describe the self-protection techniques for the user authentication mechanism (passwords are encrypted, automatically generated, are checked against a dictionary of disallowed passwords, passwords are encrypted while in transmission).
- State the number of invalid access attempts that may occur for a given user id or access location (terminal or port) and describe the actions taken when that limit is exceeded.
- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.
- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).
- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifiers, and group user identifiers) and any compensating controls.
- Describe any use of digital or electronic signatures and the standards used. Discuss the key management procedures for key generation, distribution, storage, and disposal.

**Logical Access Controls**

- Discuss the controls in place to authorize or restrict the activities of users and system personnel within the application. Describe hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists [ACLs]).
- How are access rights granted? Are privileges granted based on job function?
- Describe the application's capability to establish an ACL or register.
- Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends.
- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.
- Indicate if encryption is used to prevent access to sensitive files as part of the system or application access control procedures.
- Describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Dept. of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

**Public Access Controls**

If the public accesses the major application, discuss the additional security controls used to protect the integrity of the application and the confidence of the public in the application. Such controls include segregating information made directly accessible to the public from official agency records. Others might include:

- Some form of identification and authentication
- Access control to limit what the user can read, write, modify, or delete
- Controls to prevent public users from modifying information on the system
- Digital signatures
- CD-ROM for on-line storage of information for distribution
- Put copies of information for public access on a separate system
- Prohibit public to access "live" databases
- Verify that programs and information distributed to the public are virus-free
- Audit trails and user confidentiality
- System and data availability
- Legal considerations

**Audit Trails**

- Does the audit trail support accountability by providing a trace of user actions?
- Are audit trails designed and implemented to record appropriate information that

can assist in intrusion detection?

- Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them? (type of event, when the event occurred, user id associated with the event, program or command used to initiate the event.)
- Is access to online audit logs strictly enforced?
- Is the confidentiality of audit trail information protected if, for examples, it records personal information about users?
- Describe how frequently audit trails are reviewed and whether there are guidelines.
- Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.

# General Support System Security Plan

## SYSTEM IDENTIFICATION

Date:

### System Name/Title

- Unique Identifier and Name Given to the System

### Responsible Organization

- List organization responsible for the system

### Information Contact(s)

- Name of person(s) knowledgeable about, or the owner of, the system.

Name
Title
Address
Phone

### Assignment of Security Responsibility

- Name of person responsible for security of the system.

Name
Title
Address
Phone

### System Operational Status

If more than one status is selected, list which part of the system is covered under each status.

- Operational
- Under Development
- Undergoing a major modification

### General Description/Purpose

- Describe the function or purpose of the system and the information processed.
- Describe the processing flow of the application from system input to system output.
- List user organizations (internal and external) and type of data and processing provided.
- List all applications supported by the general support system. Describe each application's functions and information processed.

**System Environment**

- Provide a general description of the technical system. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.)
- Describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources.
- Include any security software protecting the system and information.

**System Interconnection/Information Sharing**

- List of interconnected systems and system identifiers (if appropriate).
- If connected to an external system not covered by a security plan, provide a short discussion of any security concerns that need to be considered for protection .
- It is required that written authorization (MOUs, MOAs) be obtained prior to connection with other systems and/or sharing sensitive data/information. It should detail the rules of behavior that must be maintained by the interconnecting systems. A description of these rules must be included with the security plan or discussed in this section.

**Applicable Laws or Regulations Affecting the System**

- List any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.

**General Description of Information Sensitivity**

- Describe, in general terms, the information handled by the system and the need for protective measures. Relate the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability). For each of the three categories, indicate if the requirement is: **High, Medium, or Low**.
- Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.

## MANAGEMENT CONTROLS

**Risk Assessment and Management**

- Describe the risk assessment methodology used to identify the threats and vulnerabilities of the system. Include the date the review was conducted. If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.

**Review of Security Controls**

- List any independent security reviews conducted on the system in the last three years.

- Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

**Rules of Behavior**

- A set of rules of behavior in writing must be established for each system. The rules of behavior should be made available to every user prior to receiving access to the system. It is recommended that the rules contain a signature page to acknowledge receipt.
- The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. They should state the consequences of inconsistent behavior or noncompliance. They should also include appropriate limits on interconnections to other systems.
- Attach the rules of behavior for the system as an appendix and reference the appendix number in this section or insert the rules into this section.

**Planning for Security in the Life Cycle**

Determine which phase(s) of the life cycle the system or parts of the system are in. Describe how security has been handled in the life cycle phase(s) that the system is currently in.

**Initiation Phase**

- Reference the sensitivity assessment which is described in Section 3.7, Sensitivity of Information Handled.

**Development/Acquisition Phase**

- During the system design, were security requirements identified?
- Were the appropriate security controls with associated evaluation and test procedures developed before the procurement action?
- Did the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?
- Did the requirements permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented?
- If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security requirements identified and included in the acquisition specifications?

**Implementation Phase**

- Were design reviews and systems tests run prior to placing the system in production? Were the tests documented? Has the system been certified?
- Have security controls been added since development?
- Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?
- Include the date of the certification and accreditation. If the system is not authorized yet, include date when accreditation request will be made.

**Operation/Maintenance Phase**

- The security plan documents the security activities required in this phase.

**Disposal Phase**

- Describe in this section how information is moved to another system, archived, discarded, or destroyed. Discuss controls used to ensure the confidentiality of the information.
- Is sensitive data encrypted?
- How is information cleared and purged from the system?
- Is information or media purged, overwritten, degaussed or destroyed?

**Authorize Processing**

- Provide the date of authorization, name, and title of management official authorizing processing in the system.
- If not authorized, provide the name and title of manager requesting approval to operate and date of request.

## OPERATIONAL CONTROLS

**Personnel Security**

- Have all positions been reviewed for sensitivity level?
- Have individuals received background screenings appropriate for the position to which they are assigned.
- Is user access restricted to the minimum necessary to perform the job?
- Is there a process for requesting, establishing, issuing, and closing user accounts?
- Are critical functions divided among different individuals (separation of duties)?
- What mechanisms are in place for holding users responsible for their actions?
- What are the friendly and unfriendly termination procedures?

**Physical and Environmental Protection**

- Discuss the physical protection for the system. Describe the area where processing takes place (e.g., locks on terminals, physical barriers around the building and processing area, etc.)
- Factors to address include physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, mobile and portable systems.

**Production, Input/Output Controls**

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to, software should be listed. In this section, provide a synopsis of the procedures in place that support the system. Below is a sampling of topics that should be reported in this section.

- User support - Is there a help desk or group that offers advice?

- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information
- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media
- Audit trails for receipt of sensitive inputs/outputs
- Procedures for restricting access to output products
- Procedures and controls used for transporting or mailing media or printed output
- Internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary)
- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)
- Audit trails for inventory management
- Media storage vault or library-physical, environmental protection controls/procedures
- Procedures for sanitizing electronic media for reuse (e.g., overwriting or degaussing)
- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse
- Procedures for shredding or other destructive measures for hardcopy media when no longer required

## Contingency Planning

Briefly describe the procedures (contingency plan) that would be followed to ensure the system continues to process all critical applications if a disaster were to occur. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan can be attached as an appendix.

- Any agreements of backup processing
- Documented backup procedures in including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup)
- Location of stored backups and generations of backups kept
- Are tested contingency/disaster recovery plans in place? How often are they tested?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

## Hardware and System Software Maintenance Controls

- Restriction/controls on those who perform maintenance and repair activities.
- Special procedures for performance of emergency repair and maintenance.
- Procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site).
- Procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements.

- Version control that allows association of system components to the appropriate system version.
- Procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production.
- Impact analyses to determine the effect of proposed changes on existing security controls to include the required training for both technical and user communities associated with the change in hardware/software.
- Change identification, approval, and documentation procedures.
- Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes.
- Are test data "live" data or made-up data?.
- Are there organizational policies against illegal use of copyrighted software or shareware?

**Integrity Controls**

- Is virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?
- Is reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Is password crackers/checkers used?
- Is integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?
- Are intrusion detection tools installed on the system?
- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?
- Is penetration testing performed on the system? If so, what procedures are in place to ensure they are conducted appropriately?
- Is message authentication used in the system to ensure that the sender of a message is known and that the message has not been altered during transmission?

**Documentation**

Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security of the system to include backup and contingency activities, as well as descriptions of user and operator procedures.

- List the documentation maintained for the system (vendor documentation of hardware/software, functional requirements, security plan, program manuals, test results documents, standard operating procedures, emergency procedures, contingency plans, user rules/procedures, risk assessment, authorization for processing, verification reviews/site inspections).

**Security Awareness & Training**

- The awareness program for the system (posters, booklets, and trinkets)

- Type and frequency of general support system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the job training)
- The procedures for assuring that employees and contractor personnel have been provided adequate training

**Incident Response Capability**

- Are there procedures for reporting incidents handled either by system personnel or externally?
- Are there procedures for recognizing and handling incidents, i.e., what files and logs should be kept, who to contact, and when?
- Who receives and responds to alerts/advisories, e.g., vendor patches, exploited vulnerabilities?
- What preventative measures are in place, i.e., intrusion detection tools, automated audit logs, penetration testing?

## TECHNICAL CONTROLS

**Identification and Authentication**

- Describe the method of user authentication (password, token, and biometrics).
- If a password system is used, provide the following specific information:
- Allowable character set;
- Password length (minimum, maximum);
- Password aging time frames and enforcement approach;
- Number of generations of expired passwords disallowed for use;
- Procedures for password changes;
- Procedures for handling lost passwords, and
- Procedures for handling password compromise.
- Procedures for training users and the materials covered.
- Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).
- Describe any biometrics controls used. Include a description of how the biometrics controls are implemented on the system.
- Describe any token controls used on this system and how they are implemented.
- Describe the level of enforcement of the access control mechanism (network, operating system, and application).
- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).
- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are transmitted and stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text

passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords).

- State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.
- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.
- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).
- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.
- If digital signatures are used, the technology must conforms with FIPS 186, *Digital Signature Standard* and FIPS 180-1, *Secure Hash Standard* issued by NIST, unless a waiver has been granted. Describe any use of digital or electronic signatures.

**Logical Access Controls**

- Discuss the controls in place to authorize or restrict the activities of users and system personnel within the system. Describe hardware or software features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists (ACLs).
- How are access rights granted? Are privileges granted based on job function?
- Describe the system's capability to establish an ACL or register.
- Describe how users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent user from accessing the system or applications outside of normal work hours or on weekends.
- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.
- Indicate if encryption is used to prevent access to sensitive files as part of the system or application access control procedures.
- Describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Dept. of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

**Audit Trails**

- Does the audit trail support accountability by providing a trace of user actions?
- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection?
- Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them? (type of event, when the event occurred, user id associated with the event, program or command used to initiate the event.)
- Is access to online audit logs strictly enforced?
- Is the confid entiality of audit trail information protected if, for example, it records personal information about users?
- Describe how frequently audit trails are reviewed and whether there are guidelines.
- Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem?

# Glossary

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

***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.***

***Authorize Processing*** occurs when management authorizes a system based on an assessment of management, operational and technical controls. By authorizing processing in a system the management official accepts the risk 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 toward realization of the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; and (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in automated information security.

***Certification*** is synonymous with the term **authorize processing**. 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.***)

***Confidentiality Protection*** requires access controls such as user ID/passwords, terminal identifiers, restrictions on actions like read, write, delete, etc. Examples of confidentiality-protected information are personnel, financial, proprietary, trade secrets, internal agency, investigations, other federal agency, national resources, national security, and high or new technology under Executive Order or Act of Congress.

***Designated Approving Authority (DAA)*** is the senior management official who has the authority to authorize processing (accredit) an automated information (major application) or (general support system) and accept the risk associated with the system.

***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.

***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.

***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).

***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, the assignment and limitation of system privileges, and individual accountability.

***Sensitive Information*** refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose

improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.

***Sensitivity*** in an information technology environment consists of the system, data, and applications which must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability which is determined by an evaluation of the sensitivity and criticality 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 (a) Operational - system is currently in operation, (b) Under Development - system is currently under design, development, or implementation, or (c) 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 activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.

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

# References

Guttman, Barbara and Roback, Edward. *An Introduction to Computer Security: The NIST Handbook.* Special Publication 800-12. Gaithersburg, MD: National Institute of Standards and Technology, October 1995.

NIST Computer Security Resource Clearinghouse Web site URL: http://csrc.nist.gov

Office of Management and Budget. Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources." 1996.

Public Law 100-235, "Computer Security Act of 1987."

[Schultz90] Schultz, Eugene. Project Leader, Lawrence Livermore National Laboratory. CERT Workshop, Pleasanton, CA, 1990.

Swanson, Marianne and Guttman, Barbara . *Generally Accepted Principles and Practices for Securing Information Technology Systems.* Special Publication 800-14. Gaithersburg, MD: National Institute of Standards and Technology, September 1996.

# Index