

SYSTEM SECURITY PLANS

The Service's system security plan guidance is derived from the guidance issued by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB). See the references at the end of this document. Formats for general support system (GSS) and major application security plans are posted on the Service's IT security Intranet site. The required elements for both the GSS and major application security plans are very similar. The elements are as follows:

A. Rules of behavior for the system. Rules of behavior clearly delineate responsibilities of all individuals with access to the system and include the consequences of noncompliance. The rules should clarify appropriate behavior and responsibilities when using the system. Rules for individual systems should be based on the acceptable level of risk for that system.

B. Configuration Management. Procedures to control what software is used on a system, to document changes made to the system, and to ensure that software has not been modified without proper authorization. Configuration management controls should document baseline configurations as well as procedures for testing and implementing changes to the baseline. Procedures should include the protection of software and backup copies with a combination of logical and physical access controls. Operating systems and system software that specifically support an information system (including GSS) must be documented as part of configuration management and change control procedures for the system. Controls should be documented to prevent users and systems personnel from loading and executing software on a system without authorization to reduce vulnerability to viruses, to unexpected software interactions, and to subversion or bypassing of security controls.

C. Security awareness training for system users. This training ensures that all individuals are appropriately trained on how to fulfill their security responsibilities before allowing them access to the system. Such training shall assure that employees are versed in the rules of the system, be consistent with Federal, Departmental, and Service guidance, and inform them about available assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training will be required for continued access to the system.

D. Personnel Controls. One of a set of processes used to minimize the possibility of undetected errors or irregularities by personnel who use and/or support systems. For example:

(1) Least privilege: Grant users the minimum accesses and rights they need to perform their official duties.

(2) Separation of duties: Divide the steps in a critical function among different individuals so that a single individual cannot subvert a critical process. For example, in sensitive IT systems, no single individual should normally be given authority to grant user access. Rather, one person initiates a request for access and another authorizes that access. In cases

where functions cannot be segregated, establish compensating controls by review of system administration and security administration work by knowledgeable staff. Where feasible, separation of duties should be reflected in position descriptions.

(3) Screening: If least privilege and separation of duties are not feasible, conduct background screening commensurate with the risk and magnitude of the harm they could cause prior to the individuals' being authorized to access the system and periodically thereafter. Coordinate with Human Resources to conduct the appropriate background screening for contractor staff and other non-Service personnel developing or having access to systems.

(4) Nondisclosure agreements: All contractors and other non-Service personnel must sign FWS Form 3-2235 (Nondisclosure Agreement). Provide a copy of the nondisclosure agreement to the IITSM. Retain the agreement for 1 year after termination of access.

E. Contingency plan. A contingency plan is a set of procedures established to limit the damage from events that cause harm to an information system, such as harm done by people; environmental failures such as air conditioning or electrical; or natural events such as flood or fire. Contingency plans typically mitigate harm by planning backup operations; disaster recovery of data files, hardware and/or software; alternate processing locations, power, personnel; etc. The complexity and depth of the plan depends on the degree of importance of the system relative to the functions performed and the cost of the equipment and system involved. The contingency plan must be available to all pertinent users and operators, tested whenever there are significant changes to the system, and updated as needed.

F. Identification and Authentication Controls. These controls provide base level assurance that users accessing the system are authorized to do so. Ensure that appropriate, documented security controls and procedures (such as user accounts, passwords, call back devices, encryption, data authentication, security software) are specified, designed, tested, and accepted in the system to prevent unauthorized access to or use of information, data, and software resident on computers, peripheral devices, storage media, or transmitted over communication lines or networks. These controls should provide protection consistent with the system's value and importance to Service missions. Procedures should include rules to ensure that every user has the appropriate level of access, that every account is assigned to a single individual, and that accounts are not used by others.

G. Information Sharing. Ensure that information shared between systems is protected appropriately, comparable to the protection provided when information is within the primary system.

H. System Interconnection. Obtain written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems, such as local area networks and the Service Wide Area Network (SWAN). Where connection is authorized, controls shall be established which are consistent with the rules of the system.

I. Public Access Controls. Where an agency's system promotes or permits public access, additional security controls must be added to protect the integrity of the system and the confidence the public

has in the system. Such controls will include segregating information made directly accessible to the public from official agency records.

J. Incident Response Capability. 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 with other bureaus and organizations, consistent with FedCIRC coordination. Provide instructions for document and reporting incidents to the appropriate individuals.

K. Risk Assessment. Evaluate system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events and the identification of mitigating countermeasures. Risk assessment should be commensurate to the size and complexity of the system and provide management valuable information to be used in allocating and managing scarce resources. A risk assessment should be accomplished whenever a new system is developed, significantly modified or changed, or every 3 years, whichever occurs first. A risk assessment might also be triggered by external changes that affect the security of operating systems. The depth and complexity of the analysis is in proportion to the system being evaluated. At a minimum, the risk assessment should:

- (1) Identify threats that could damage the system and/or its ability to provide required support, for example fire, theft, computer virus, etc.
- (2) Identify vulnerabilities in the system, such as lack of fire protection equipment.
- (3) Identify risks as cases where there is a vulnerability that could result in harm from a threat, for example the threat of damage from fire together with the vulnerability of a lack of fire protection equipment.
- (4) Evaluate the potential for loss and advise management so that cost effective countermeasures can be implemented.

References:

NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook"

NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems"

NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems"

OMB Circular A-130, Appendix III

Department of the Interior - Information Technology Security Plan