APPENDIX IV

INFORMATION TECHNOLOGY SECURITY GUIDELINES[1]

1 The information in this appendix is attributed to National Institute of Standards and Technology (NIST) Special Publications (SP) and Federal Information Processing Standards (FIPS). These publications can be found on the NIST website, http://csrc.nist.gov/publications/PubsSPs.html, and http://csrc.nist.gov/publications/PubsFIPS.html, respectively. Web links of the key NIST documents are provided below:

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems, 2006 February;*
NIST SP 800-30, *Risk Management Guide for Information Technology Systems, 2002 July;*
NIST SP 800-34, *Contingency Planning for Information Technology Systems, 2002 June;*
NIST SP 800-100, *Information Security Handbook: A Guide for Managers, 2006 October;*
FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems, 2004 February;*
FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems, 2006 March;*

INFORMATION TECHNOLOGY (IT) CONTINGENCY PLANNING

Contingency planning for information systems is a required process for developing general support systems (GSS) and major applications (MA) with appropriate backup methods and procedures for implementing data recovery and reconstitution against IT risks. Risks to information systems may be natural, technological, or human in nature.

Contingency planning refers to interim measures to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

The capability to recover and reconstitute data should be integral to the information system design concept during the Initiation phase of Software Development Life Cycle of a system. Recovery strategies should be built into the architecture of the system during the Development phase. The contingency processes should be tested and maintained during the Implementation phase; contingency plans should be exercised and maintained during the Operations/Maintenance phase.

NIST SP 800-34, *Contingency Planning for Information Technology Systems*, details a seven-step methodology for developing an IT contingency process and plan. These seven steps are summarized below:

Step 1: Develop Contingency Planning Policy Statement

A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan. The statement should define the agency's overall contingency objectives; identify leadership, roles and responsibilities, resource requirements, test, training, and exercise schedules; and develop maintenance schedules and determine the minimum required backup frequency.

Step 2: Conduct Business Impact Analysis

A business impact analysis (BIA) is a critical step to understanding the information systems components, interdependencies, and potential downtime impacts. The BIA helps to identify and prioritize critical IT systems and components. Contingency plan strategy and procedures should be designed in consideration of the results of the BIA.

A BIA is conducted by identifying the system's critical resources. Each critical resource is then further examined to determine how long functionality of the resource could be withheld from the information system before an unacceptable impact is experienced. The impact may be something that materializes over time or may be tracked across related resources and dependent systems (e.g., cascading domino effect). The time identified is

called a maximum allowable outage (MAO). Based on the potential impacts, the amount of time the information system can be without the critical resource then provides a recourse recovery priority around which an organization can plan recovery activities. The balancing point between the MAO and the cost to recover establishes the information system's recovery time objective (RTO). Recovery strategies must be created to meet the RTO. The strategy must also address recovering information system critical components within a priority, as established by their individual RTOs.

Step 3: Identify Preventive Controls

In some cases, implementing preventive controls might mitigate outage impacts identified by the BIA. Preventive controls are measures that detect, deter, and/or reduce impacts to the system. When cost-effective, preventing an impact is desired over implementing recovery strategies (and therefore risking data loss and impact to the organization). Preventive measures are specific to individual components and the environment in which the components operate. Common controls include:

- Uninterruptible power supply (UPS);
- Fire suppression systems;
- Gasoline or diesel-powered generators;
- Air conditioning systems with excess capacity to permit failure of certain components;
- Heat-resistant and waterproof containers for backup media and vital non-electronic records; and
- Frequent, scheduled data backups.

Step 4: Develop Recovery Strategies

When a disruption occurs despite the preventive measures implemented, a recovery strategy must be in place to recover and restore data and system operations within the RTO period. The recovery strategy is designed from a combination of methods, which together address the full spectrum of information system risks. The most cost-effective option, based on potential impact, should be selected and integrated into the information system architecture and operating procedures.

System data must be backed up regularly; therefore, all IT contingency plans should include a method and frequency for conducting data backups based on system criticality. Data that is backed up may need to be stored offsite and rotated frequently, depending upon the criticality of the system.

Major disruptions to system operations may require restoration activities to be implemented at an alternate site. The type of alternate site selected must be based on RTO requirements and budget limitations. Equipment for recovering and/or replacing the information system must be provided as part of the recovery strategy. Cost, delivery time, and compatibility factors must also be considered when determining how to provide the necessary equipment. Agencies must also plan for an alternate site that, at a

minimum, provides workspace for all contingency plan personnel, equipment, and the appropriate IT infrastructure necessary to execute IT contingency plan and system recovery activities.

The recovery strategy requires personnel to implement the procedures and test operability. Generally, a member of the organization's senior leadership is selected to activate the plan and lead overall recovery operations. Appropriate teams of personnel (at least two people to ensure there is a primary and alternate available to execute procedures) are identified to be responsible for specific aspects of the plan. Personnel should be chosen to staff the teams based on their normal responsibilities, system knowledge, and availability to recover the system on an on-call basis. A line of succession should be defined to ensure that someone could assume the role of senior leadership if the plan leader is unable to respond.

Step 5: Develop IT Contingency Plan

Procedures for executing the recovery strategy are outlined in the IT contingency plan. The plan must be written in a format that will provide the users (recovery team leadership and members) the context in which the plan is to be implemented and the direct procedures, based on role, to execute.

The NIST SP 800-34, *Contingency Planning for Information Technology Systems* presents a sample format for developing an IT contingency plan. The format defines three main phases that govern the actions to be taken following a system disruption. The **Notification/Activation** phase describes the process of notifying recovery personnel and performing a damage assessment. The **Recovery** phase discusses a suggested course of action for recovery teams and personnel to restore IT operations at an alternate site or using contingency capabilities. The final phase, **Reconstitution**, outlines actions that can be taken to return the system to normal operating conditions. Additionally, the format contains the Supporting Information and Appendices components, which provide supplemental information necessary to understand the context in which the plan is to be used and gives additional information that, may be necessary to execute procedures (e.g., emergency contact information and the BIA).

Step 6: Plan Testing, Training, and Exercises

Personnel selected to execute the IT contingency plan must be trained to perform the procedures, the plan must be exercised, and the system strategy must be tested.

Plan testing should include:

• System recovery on an alternate platform from backup media	• System performance using alternate equipment
• Coordination among recovery teams	• Restoration of normal operations
• Internal and external connectivity	• Notification procedures

Personnel training should include:

• Purpose of the plan	• Security requirements
• Cross-team coordination and communication	• Team-specific processes
• Reporting procedures	• Individual responsibilities

Plan exercises should be designed to examine, individually and then collectively, various components of the entire plan. Exercises may be conducted in a classroom setting: discussing specific components of the plan and/or impact issues; or they may be functional exercises: simulating the recovery using actual replacement equipment, data, and alternate sites.

Step 7: Plan Maintenance

The IT contingency plan must always be maintained in a ready state for use immediately upon notification. At least, annual reviews of the plan must be conducted to ensure that key personnel and vendor information, system components and dependencies, the recovery strategy, vital records, and operational requirements are up to date. While some changes may be obvious (e.g., personnel turnover or vendor changes), others will require analysis. The BIA should be reviewed periodically and updated with new information to identify new contingency requirements and priorities. Changes made to the plan are noted in a record of changes, dated, and signed or initialed by the person making the change. The revised plan, or plan sections are circulated to those with plan responsibilities. Because of the impact that plan changes may have on interdependent business processes or information systems, the changes must be clearly communicated and properly annotated in the beginning of the document.

Risk Management

An effective risk management process is an important component of a successful information security program. The principal goal of an organization's risk management process is to protect the organization and its ability to perform its mission, not just its information assets. Risk Management is an essential management function of the organization that is tightly woven into the system development life cycle (SDLC). Because risk cannot be eliminated entirely, the risk management process allows information security program managers to balance the operational and economic costs of protective measures and achieve gains in mission capability. By employing practices and procedures designed to foster informed decision-making, agencies help protect their information systems and the data that support their own mission.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, provides for the development of an effective risk management program.

Risk management is an aggregation of three processes:

1. Risk Assessment,
2. Risk Mitigation, and
3. Evaluation and Assessment.

These three processes are summarized below:

Risk Assessment

The goal of the risk assessment process is to identify and assess the risks to a given environment. The depth of the risk assessment performed can vary greatly and is determined by the criticality and sensitivity of the system, as applied to confidentiality, integrity, and availability. To meet the goal of the risk assessment, a process is divided into following steps:

Step 1: System Characterization

Characterizing an information system establishes the scope of the risk assessment effort, delineates the operational authorization boundaries, and provides information. This step begins with the identification of the information system boundaries, resources, and information.

When characterizing the system, the mission criticality and sensitivity are described in sufficient terms to form a basis for the scope of the risk assessment. Various techniques, such as questionnaires, interviews, documentation reviews, and automated scanning tools, can be used to collect the information needed to characterize the system completely. At a minimum, the system characterization describes the following individual system components:

- Hardware;
- Software;
- External interfaces to other systems;
- Data; and
- People.

In addition to the component descriptions, the system characterization describes other factors with the potential to affect the security of the system, such as:

- System functional requirements;
- Organizational security policy and architecture;
- System network topology;
- Information flows throughout the system;
- Management, operational, and technical security controls implemented or planned to be implemented for the system; and
- Physical and environmental security mechanisms.

Step 2: Threat Identification

Threat identification consists of identifying threat sources with the potential to exploit weaknesses in the system. The threat statement must be tailored to the individual organization and its processing environment (e.g., end-user computing habits), which is accomplished by performing a threat evaluation, using the system characterization as the basis, for the potential to cause harm to the system.

There are common threat sources that typically apply, regardless of the system, and should be evaluated. These common threats can be categorized into three areas:

- Natural threats (e.g., floods, earthquakes, tornadoes, landslides, avalanches, electrical storms),
- Human threats (intentional or unintentional), and
- Environmental threats (e.g., power failure).

In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available, as known threats have been identified by many government and private sector organizations. Intrusion detection tools also are becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to assess threats realistically.

Step 3: Vulnerability Identification

Vulnerability is defined as "a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy". Vulnerabilities can be identified using a combination of a number of

techniques and sources. Reviews of such sources as previous risk assessments, audit reports, vulnerability lists, and security advisories can be used to begin the process of vulnerability identification. System security testing, using methods such as automated vulnerability scanning tools; security, test, and evaluation (ST&E); and penetration testing can be used to augment the vulnerability source reviews and identify vulnerabilities that may not have been previously identified in other sources.

In addition, developing a security requirements checklist based on the security requirements specified for the system during the conceptual, design, and implementation phases of the SDLC can be used to provide a 360-degree inspection of the system. The checklist developed must ensure the inclusion of appropriate questions in the areas of management, operational and technical security controls. The results of the checklist can be used as input for evaluating compliance and noncompliance, which in turn identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

Step 4: Risk Analysis

The risk analysis is a determination (or estimation) of risk to the system, an analysis that requires the consideration of closely interwoven factors, such as the security controls in place for the system under review, the likelihood that those controls will be either insufficient or ineffective protection of the system, and the impact of that failure. The following four steps—control analysis, likelihood determination, impact analysis, and risk determination—are, in a practical sense, performed simultaneously or nearly simultaneously because they are so tightly linked to each other.

1. Control Analysis

As previously discussed, the analysis of controls in place to protect the system can be accomplished using a checklist or questionnaire, which is based on the security requirements for the system. The checklist also provides guidance on testing security controls. The results are used to strengthen the determination of the likelihood that a specific threat might successfully exploit a particular vulnerability.

2. Likelihood Determination

Likelihood determination considers a threat source's motivation and capability to exploit vulnerability, the nature of the vulnerability, the existence of security controls, and the effectiveness of mitigating security controls. Likelihood ratings are described in the qualitative terms of high, moderate, and low, and are used to describe how likely a successful exploitation of a vulnerability is by a given threat. For example, if a threat is highly motivated and sufficiently capable, and controls implemented to protect the vulnerability are ineffective, then it is highly likely that the attack would be successful. In this scenario, the appropriate likelihood rating would be high. The likelihood ratings of moderate and low are similarly defined to successively lesser degrees.

3. Impact Analysis

The third factor used in determining the level of risk to a system is impact. A proper overall impact analysis considers the following factors: impact to the systems, data, and the organization's mission. Additionally, this analysis should also consider the criticality and sensitivity of the system and its data for the three security domains of confidentiality, integrity, and availability. Tools such as mission-impact reports, asset criticality assessment reports, and business impact analyses results in a rating describing the estimated impact to the system and organization should a threat successfully exploit vulnerability. While impact can be described using either a quantitative or qualitative approach, in the context of information technology (IT) systems and data, impact is generally described in qualitative terms. As with the ratings used to describe likelihood, impact levels are described using the terms of high, moderate, and low. NIST SP 800-30 provides definitions for the impact ratings of low, medium, and high.

4. Risk Determination

Once the ratings for likelihood and impact have been determined through appropriate analyses, the level of risk to the system and the organization can be derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. NIST SP 800-30 provides how to calculate an overall risk rating using inputs from the threat likelihood and impact categories.

Step 5: Control Recommendations

The goal of the control recommendations is to reduce the level of risk to the information system and its data to a level the organization deems acceptable. These recommendations are essential input for the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented. This step is designed to help agencies identify and select controls appropriate to the organization's operations and mission that could mitigate or eliminate the risks identified in the preceding steps. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

Effectiveness of recommended options (e.g., system compatibility):

- Legislation and regulation;
- Organizational policy;
- Operational impact; and
- Safety and reliability.

Step 6: Results Documentation

The risk assessment report is the mechanism used to report the results formally of all

risk assessment activities. The intended function of this report is to describe and document the risk posture of the system while it is operating in its stated environment (as described in the system characterization) and to provide organization managers with sufficient information so that they can make sound, risk-based decisions, such as resources that must be allocated to the risk mitigation phase. Lastly, the agency should ensure that the results of the risk assessment are appropriately reflected in the system's Plan of Action and Milestones (POA&M) and System Security Plan.

At a minimum, the risk assessment report should describe the following:

- Scope of the assessment based on the system characterization;
- Methodology used to conduct the risk assessment;
- Individual observations resulting from conducting the risk assessment; and
- Estimation of the overall risk posture of the system.

The risk assessment process is usually repeated at least every three years. However, risk assessments should be conducted and integrated into the SDLC for information systems.

Risk Mitigation

The second phase of the risk management process is risk mitigation. Because it is impractical, if not impossible, to eliminate all risk from a system, risk mitigation strives to prioritize, evaluate, and implement the appropriate risk-reducing controls recommended from the risk assessment process. Managers may use several options to reduce the risk to a system. These options are risk assumption; risk avoidance; risk limitation; risk planning, research, and acknowledgement; and risk transference.

A straightforward strategy can be used to determine whether risk mitigation actions are necessary. Working from each risk identified and analyzed in the first process—risk assessment—managers must then decide whether the risk is acceptable or unacceptable and, subsequently, whether to implement additional controls or not to mitigate unacceptable risks. Once the decision has been made on which risks are to be addressed in the risk mitigation process, a seven-step approach is used to guide the selection of security controls:

1. Prioritize actions;
2. Evaluate recommended control options;
3. Conduct cost-benefit analyses;
4. Select controls;
5. Assign responsibility;
6. Develop a safeguard implementation plan; and
7. Implement selected control(s).

The process of selecting controls to mitigate identified risks to an acceptable level is based on the security categorization of the system. For new systems, once the security controls for the system have been identified and refined and an initial risk assessment

conducted, the selected controls must be implemented. For legacy systems, the security controls that are selected are verified.

Organizations can leverage controls used among multiple systems by designating them as common controls where implementation, assessment, and monitoring is conducted at an organizational level or by areas of specific expertise (e.g., human resources, physical security, building management). The system owner must understand who is responsible for implementing these controls and identify the risk that this extension of trust will generate.

Because it is impracticable to eliminate all risk, it is important to note that even after the controls have been selected and implemented, some degree of residual risk will remain. The remaining residual risk should be analyzed to ensure that it is at an acceptable level. After the appropriate controls have been put in place for the identified risks, the authorizing official should sign a statement accepting any residual risk. Either the official should authorize the operation of the new information system or request continued processing of the existing information system. If the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a way of lowering the residual risk to an acceptable level.

Evaluation and Assessment

The third and final phase in the risk management process is evaluation and assessment. The art of risk management in today's dynamic and constantly changing IT environments must be ongoing and continuously evolving. Systems are upgraded and expanded, components are improved, and architectures are constantly evolving.

The evaluation and assessment of security controls' effectiveness must be performed. The results are used to provide an Authorizing Official with the essential information needed to make a credible, risk-based decision on whether to authorize the operation of the information system. The reuse of assessment data will not only save valuable resources, but also provide the most up-to-date risk information for the authorizing official.

Many of the risk management activities are conducted during a snapshot in time—a static representation of a dynamic environment. All the changes that occur to systems during normal, daily operations have the potential to affect the security of the system adversely in some fashion, and it is the goal of the risk management evaluation and assessment process to ensure that the system continues to operate in a safe and secure manner. This goal can be partially reached by implementing a strong configuration management program. In addition to monitoring the security of an information system on a continuous basis, agencies must track findings from the security control assessment to ensure they are addressed appropriately and do not continue to pose or introduce new risks to the system.

System Security Planning

The objective of system security planning is to improve the protection of information system resources. The protection of a system must be documented in a system security plan. The purpose of the system 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. It should reflect input from various managers with responsibilities concerning the system.

NIST SP 800-18 *Guide for Developing Security Plans for Federal Information Systems*, provides basic information on how to prepare a system security plan in accordance with applicable federal requirements, and it is easily adaptable to a variety of organizational structures.

Program managers, system owners, and security personnel in the organization must understand the system security planning process. In addition, users of the information system and those responsible for defining system requirements should also be familiar with the system security planning process, as the system security plan is an important deliverable in the SDLC process. Those responsible for implementing and managing information systems must participate in addressing security controls to be applied to their systems.

Applications

All information systems must be covered by a system security plan. Systems can be labeled as a major application (MA) or general support system (GSS). MA is defined as an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. GSS is defined as an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. A minor application is an application, other than major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a GSS.

Security Planning Roles and Responsibilities

Agencies should develop policy on the system security planning process. System security plans are living documents that require periodic review, modification, and plans of action and milestones (POA&M) for implementing security controls. Procedures should be in place outlining who reviews the plans, keeps the plan current, and follows up on planned security controls.

The roles and responsibilities in this section are specific to information system security planning.

Chief Information Officer

The chief information officer (CIO) is the agency official responsible for developing and maintaining an agency-wide information security program and has the following system security planning responsibilities:

Designating a Senior Agency Information Security Officer (SAISO) who shall carry out the CIO's responsibilities for system security planning such as:

- Developing and maintaining information security policies, procedures, and control techniques to address system security planning;
- Managing the identification, implementation, and assessment of common security controls;
- Ensuring that personnel with significant responsibilities for system security plans are trained;
- Assisting senior agency officials with their responsibilities for system security plans; and
- Identifying and developing common security controls for the agency.

Information System Owner

The information system owner is the agency official responsible for the overall procurement, development, integration, modification, and operation and maintenance of the information system. The information system owner has the following responsibilities related to system security plans:

- Developing the system security plan in coordination with information owners, the system administrator, the information system security officer (ISSO), the SAISO, and functional "end users";
- Maintaining the system security plan and ensuring that the system is deployed and operated according to the agreed-upon security requirements; and
- Ensuring that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior) and assisting in the identification, implementation, and assessment of the common security controls.

Information Owner

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

- Establishing the rules for the appropriate use and protection of the subject data/information (rules of behavior);
- Providing input to information system owners on the security requirements and security controls for the information systems where the information resides;
- Deciding who has access to the information system and determining what types of privileges or access rights; and
- Assisting in identifying and assessing the common security controls where the information resides.

Senior Agency Information Security Officer

The SAISO is the agency official responsible for serving as the CIO's primary liaison to the agency's information system owners and ISSOs. The SAISO has the following responsibilities related to system security plans:

- Carrying out the CIO's responsibilities for system security planning;
- Coordinating the development, review, and acceptance of system security plans with information system owners, ISSOs, and the authorizing official;
- Coordinating the identification, implementation, and assessment of the common security controls; and
- Possessing professional qualifications, including training and experience, required to develop and review system security plans.

Information System Security Officer

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

- Assisting the SAISO in identifying, implementing, and assessing the common security controls; and
- Actively supporting the development and maintenance of the system security plan, to include coordinating system changes with the information system owner and assessing the security impact of those changes.

Rules of Behavior

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 and be made available to every user prior to receiving authorization for system access. It is required that the rules contain a signature page for each user to acknowledge receipt, indicating that they have read, understand, and agree to abide by the rules of behavior. Electronic signatures are acceptable for use in acknowledging the rules of behavior.

Following lists the examples of what should be covered in typical rules of behavior:

- Delineate responsibilities, expected use of system, and behavior of all users
- Describe appropriate limits on interconnections
- Define service provisions and restoration priorities
- Be clear on consequences of behavior not consistent with rules

It covers the following topics:

- Work at home
- Dial-in access
- Connection to the Internet
- Use of copyrighted work
- Unofficial use of government equipment
- Assignment and limitations of system privileges and individual accountability
- Password usage
- Searching databases and divulging information

Agencies can incorporate, by reference, the agency body of policies and procedures governing information security and other applicable policies in the text of the rules of behavior.

System Security Plan Approval

Organizational policy should clearly define who is responsible for system security plan approval and procedures developed for plan submission, including any special memorandum language or other documentation required by the agency.

System Boundary Analysis and Security Controls

Before the system security plan is developed, the information system as well as the information itself should be categorized based on impact analysis. NIST issued FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* to develop standards for categorizing information and information systems. Refer to FIPS Publication 199 for more information on system categorization. Then a determination can be made as to which systems in the inventory can be logically grouped into GSSs or MAs. The FIPS 199 impact levels should be considered when the system boundaries are drawn and when selecting the initial set of security controls (e.g., control baseline). The baseline security controls can then be tailored based on an assessment of risk and local conditions, including organization-specific security requirements, specific threat information, cost-benefit analyses, the availability of compensating controls, or special circumstances. Common security controls, which is one of the tailoring considerations, must be identified prior to system security plan preparation to identify those controls covered at the agency level that are not system-specific. These common security controls can then be incorporated into the system security plan by reference.

Security Controls

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* provides seventeen minimum-security requirements for the information systems. The requirements represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting the confidentiality, integrity, and availability of the information and information systems. An agency should meet the minimum-security requirements in this standard by applying security controls selected in accordance with NIST SP 800-53, *Recommended Security Control for Federal Information Systems* and the designated impact levels of the information systems. An agency has the flexibility to tailor the security control baseline in accordance with the terms and conditions set forth in the standard. Tailoring activities include:

(1) the application of scoping guidance,
(2) the specification of compensating controls, and
(3) the specification of agency-defined parameters in the security controls, where allowed. The system security plan should document all tailoring activities.

Scoping Guidance

Scoping guidance provides an agency with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines defined in NIST SP 800-53. System security plans should clearly identify which security controls used scoping guidance. In addition, system security plans should include a description of the type of considerations that were made.

Compensating Controls

Compensating security controls are the management, operational, or technical controls used by an agency in lieu of prescribed controls in the low, moderate, or high security control baselines, which provide equivalent or comparable protection for an information system. Compensating security controls for an information system should be used by an agency only under the following conditions:

(1) The agency selects the compensating controls from the security control catalog in NIST SP 800-53;
(2) The agency provides a full and complete rationale and justification for how the compensating controls provide an equivalent security capability or level of protection for the information system; and
(3) The agency assesses and formally accepts the risk associated with using the compensating controls in the information system.

Common Security Controls

An agency-wide view of the information security program facilitates the identification of common security controls that can be applied to one or more agency information systems.

Common security controls can apply to all agency information systems; a group of information systems at a specific site; or common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites. Common security controls are typically identified during a collaborative agency-wide process that involves the CIO, SAISO, authorizing officials, information system owners, and ISSOs.

For efficiency in developing system security plans, common security controls should be documented once and then inserted or imported into each system security plan for the information systems within the agency.

Security Control Selection

An agency should meet the minimum-security requirements in FIPS 199 by selecting the appropriate security controls and assurance requirements as described in NIST SP 800-53. The process of selecting the appropriate security controls and assurance requirements for agency information systems to achieve adequate security is a multifaceted, risk-based activity involving management and operational personnel within the agency. Subsequent to the security categorization process, an agency must select an appropriate set of security controls for their information systems that satisfy the minimum-security requirements set forth in FIPS 200. The selected set of security controls must be one of three security control baselines from NIST SP 800-53 (see Table below) that are associated with the designated impact levels of the agency information systems as determined during the security categorization process.

FIPS 199 Categorization

Potential Impact			
Security Objective	**Low**	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and	The disruption of access to or use of information or an information system could be	The disruption of access to or use of information or an information system could be	The disruption of access to or use of information or an information system could be

reliable access to and use of information. [44 U.S.C., SEC. 3542]	expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Completion and Approval Dates

The completion date of the system security plan should be provided. The completion date should be updated whenever the plan is periodically reviewed and updated. The system security plan should also contain the date the authorizing official or the designated approving authority approves the plan.

Ongoing System Security Plan Maintenance

Once the information system security plan is approved, it is important to periodically assess the plan; review any change in system status, functionality, design, etc.; and ensure that the plan continues to reflect the correct information about the system. This documentation and its accuracy are imperative for system recertification and reaccreditation activity. All plans should be reviewed and updated, if appropriate, at least annually. Some items to include in the review are:

- Change in information system owner;
- Change in information security representative;
- Major change in system architecture;
- Change in system status;
- Additions/deletions of system interconnections;
- Change in system scope; and
- Change in authorizing official.

SAMPLE PLAN FORMATS

SAMPLE IT CONTINGENCY PLAN FORMAT

This sample format provides a template for preparing an information technology (IT) contingency plan. The template is intended to be used as a guide, and the Contingency Planning Coordinator should modify the format as necessary to meet the system's contingency requirements and comply with internal policies. Where practical, the guide provides instructions for completing specific sections. Text is added in certain sections; however, this information is intended only to suggest the type of information that may be found in that section. The text is not comprehensive and should be modified to meet specific agency and system considerations. The IT contingency plan should be marked with the appropriate security label, such as *Official Use Only*.

1IT CONTINGENCY PLAN

2

31. INTRODUCTION

4

51.1 PURPOSE

This {*system name}* Contingency Plan establishes procedures to recover the {*system name}* following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - *Notification/Activation phase* to detect and assess damage and to activate the plan
  - *Recovery phase* to restore temporary IT operations and recover damage done to the original system
  - *Reconstitution phase* to restore IT system-processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out {*system name}* processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated *{Organization name}* personnel and provide guidance for recovering {*system name}* during prolonged periods of interruption to normal operations.
- Ensure coordination with other *{Organization name}* staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

0

21.2 APPLICABILITY

The {*system name}* Contingency Plan applies to the functions, operations, and resources necessary to restore and resume {*Organization name}'s* {*system name}* operations as it is installed at *primary location name, City, State*. The {*system name}* Contingency Plan applies to *{Organization name}* and all other persons associated with *{system name}* as identified under Section 2.3, Responsibilities.
The *{system name}* Contingency Plan is supported by *plan name,* which provides the *purpose of plan.* Procedures outlined in this plan are coordinated with and support the *plan name*, which provides *purpose of plan.*

1

21.3 SCOPE

31.3.1 Planning Principles

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles:

- *The {Organization name}'s* facility in *City, State,* is inaccessible; therefore, *{Organization name}* is unable to perform {*system name}* processing for the *Department*.
- A valid contract exists with the alternate site that designates that site in City, State, as the {Organization name}'s alternate operating facility.
  - {Organization name} will use the alternate site building and IT resources to recover {system name} functionality during an emergency that prevents access to the original facility.
  - The designated computer system at the alternate site has been configured to begin processing {system name} information.
  - The alternate site will be used to continue {system name} recovery and processing throughout the period of disruption, until the return to normal operations.

11.3.2 Assumptions

Based on these principles, the following assumptions were used when developing the IT Contingency Plan:

- The {system name} is inoperable at the {Organization name} computer center and cannot be recovered within 48 hours.
- Key {system name} personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the {system name} Contingency Plan.
- Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are operational at the time of the disaster.
- Computer center equipment, including components supporting {system name}, are connected to an uninterruptible power supply (UPS) that provides 45 minutes to 1 hour of electricity during a power failure.
- {system name} hardware and software at the {Organization name} original site are unavailable for at least 48 hours.
- Current backups of the application software and data are intact and available at the offsite storage facility.
- The equipment, connections, and capabilities required to operate {system name} are available at the alternate site in City, State.
- Service agreements are maintained with {system name} hardware, software, and communications providers to support the emergency system recovery.

The {system name} Contingency Plan does not apply to the following situations:

- **Overall recovery and continuity of business operations.** The Business Resumption Plan (BRP) and Continuity of Operations Plan (COOP) are appended to the plan.
- **Emergency evacuation of personnel.** The Occupant Evacuation Plan (OEP) is appended to the plan.
- *Any additional constraints should be added to this list.*

0

21.4 REFERENCES/REQUIREMENTS

This {system name} Contingency Plan complies with the {Organization name}'s IT contingency planning policy as follows:

The organization shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 72 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

The {system name} Contingency Plan also complies with the following federal and departmental policies:

- The Computer Security Act of 1987
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.
- Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations, July 1999
- Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations, October 1998
- PDD 63, Critical Infrastructure Protection, May 1998
- Federal Emergency Management Agency (FEMA), The Federal Response Plan (FRP), April 1999
- Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, "Government Information Security Reform," October 30, 2000
- Any other applicable federal policies should be added
- Any other applicable departmental policies should be added.

1.5 RECORD OF CHANGES

Modifications made to this plan since the last printing are as follows:

Record of Changes			
Page No.	**Change Comment**	**Date of Change**	**Signature**

12. CONCEPT OF OPERATIONS

2.1 SYSTEM DESCRIPTION AND ARCHITECTURE

Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including security controls and telecommunications connections.

1

2.2 LINE OF SUCCESSION

The *{organization name}* sets forth an order of succession, in coordination with the order set forth by the *department* to ensure that decision-making authority for the {*system name*} Contingency Plan is uninterrupted. The Chief Information Officer (CIO), {*organization name*} is responsible for ensuring the safety of personnel and the execution of procedures documented within this {*system name*} Contingency Plan. If the CIO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Deputy CIO shall function as that authority. *Continue description of succession as applicable.*

1

22.3 RESPONSIBILITIES

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

The Contingency Plan establishes several teams assigned to participate in recovering *{system name}* operations. The *{team name}* is responsible for recovery of the *{system name}* computer environment and all applications. Members of the *team name* include personnel who are also responsible for the daily operations and maintenance of *{system name}*. The *team leader title* directs the *{team name}.*

Continue to describe each team, their responsibilities, leadership, and coordination with other applicable teams during a recovery operation.

The relationships of the team leaders involved in *system* recovery and their member teams are illustrated in Figure XX below.

> *(Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel.)*

Describe each team separately, highlighting overall recovery goals and specific responsibilities. Do not detail the procedures that will be used to execute these responsibilities. These procedures will be itemized in the appropriate phase sections.

3. NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a

disruption to {*system name*}. Based on the assessment of the event, the plan may be activated by the Contingency Planning Coordinator.

> **In an emergency, the {*Organization name*}'s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.**

Contact information for key personnel is located in Personnel Contact list appendix. The notification sequence is listed below:

- The first responder is to notify the *Contingency Planning Coordinator*. All known information must be relayed to the *Contingency Planning Coordinator*.
- The systems manager is to contact the *Damage Assessment Team Leader* and inform them of the event. The *Contingency Planning Coordinator* is to instruct the *Team Leader* to begin assessment procedures.
- The *Damage Assessment Team Leader* is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the *Damage Assessment Team* is to follow the outline below.

Damage Assessment Procedures:

(Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations.)

- Upon notification from the *Contingency Planning Coordinator*, the *Damage Assessment Team Leader* is to …
- The *Damage Assessment Team* is to ….

Alternate Assessment Procedures:

- Upon notification from the *Contingency Planning Coordinator*, the *Damage Assessment Team Leader* is to …
- The *Damage Assessment Team* is to ….

1− When damage assessment has been completed, the *Damage Assessment Team Leader* is to notify the *Contingency Planning Coordinator* of the results.

2− The *Contingency Planning Coordinator* is to evaluate the results and determine whether the contingency plan is to be activated and if relocation is required.

3− Based on assessment results, the *Contingency Planning Coordinator* is to notify assessment results to civil emergency personnel (e.g., police, fire) as appropriate.

The Contingency Plan is to be activated if one or more of the following criteria are

met:

11. {*System name*} will be unavailable for more than 48 hours
22. Facility is damaged and will be unavailable for more than 24 hours
33. Other criteria, as appropriate.

- If the plan is to be activated, the *Contingency Planning Coordinator* is to notify all Team Leaders and inform them of the details of the event and if relocation is required.
- Upon notification from the *Contingency Planning Coordinator*, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The *Contingency Planning Coordinator* is to notify the *off-site storage facility* that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the *alternate site*.
- The *Contingency Planning Coordinator* is to notify the Alternate site that a contingency event has been declared and to prepare the facility for the *Organization's* arrival.
- The *Contingency Planning Coordinator* is to notify remaining personnel (via notification procedures) on the general status of the incident.

1

24. RECOVERY OPERATIONS

This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities. The following procedures are for recovering the {*system name*} at *the alternate site*. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal. *State the first recovery objective as determined by the Business Impact Assessment (BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.*

- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*

Recovery Goal. *State the second recovery objective as determined by the BIA. For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.*

- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*

- *Team Recovery Procedures*

- *{team name}*
  - *Team Recovery Procedures*

Recovery Goal. *State the remaining recovery objectives (as determined by the BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.*

1

25. RETURN TO NORMAL OPERATIONS

This section discusses activities necessary for restoring {*system name*} operations at the {*Organization name*}'s original or new site. When the computer center at the original or new site has been restored, {*system name*} operations at the alternate site must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

Original or New Site Restoration

Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested.

- *{team name}*
  - *Team Resumption Procedures*
- *{team name}*
  - *Team Resumption Procedures*

1

25.1 CONCURRENT PROCESSING

Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.

- *{team name}*
  - *Team Resumption Procedures*
- *{team name}*
  - *Team Resumption Procedures*

1

25.2 PLAN DEACTIVATION

Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s). Team members should be instructed to return to the original or new site.

- *{team name}*
  - *Team Testing Procedures*
- *{team name}*
  - *Team Testing Procedures*

1

26. PLAN APPENDICES

The appendices included should be based on system and plan requirements.

- Personnel Contact List
- Vendor Contact List
- Equipment and Specifications
- Service Level Agreements and Memorandums of Understanding
- IT Standard Operating Procedures
- Business Impact Analysis
- Related Contingency Plans
- Emergency Management Plan
- Occupant Evacuation Plan
- Continuity of Operations Plan.

Sample Information System Security Plan Template

The following sample has been provided ONLY as one example. Agencies may be using other formats and choose to update those to reflect any existing omissions based on this guidance. This is not a mandatory format; it is recognized that numerous agencies and information security service providers may have developed and implemented various approaches for information system security plan development and presentation to suit their own needs for flexibility. The template instructions, which are separate from the template, will assist the user when completing the sections of the plan.

Information System Security Plan

1. Information System Name/Title:
2. Information System Categorization:

	LOW		**MODERATE**		**HIGH**

3. Information System Owner:
4. Authorizing Official:
5. Other Designated Contacts:
6. Assignment of Security Responsibility:
7. Information System Operational Status:

	Operational		**Under Development**		**Major Modification**

8. Information System Type:

	Major Application		**General Support System**

9. General System Description/Purpose

10. System Environment

11. System Interconnections/Information Sharing

System Name	Organization	Type	Agreement (ISA/MOU/MOA)	Date	FIPS 199 Category	C&A Status	Auth. Official

12. Related Laws/Regulations/Policies

13. Minimum Security Controls

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

14. Information System Security Plan Completion Date: _____

15. Information System Security Plan Approval Date: _____

Template Instructions

1. Information System Name/Title

- Unique identifier and name given to the system.

2. Information System Categorization

- Identify the appropriate FIPS 199 categorization.

3. Information System Owner

- Name, title, agency, address, email address, and phone number of person who owns the system.

4. Authorizing Official

- Name, title, agency, address, email address, and phone number of the senior management official designated as the authorizing official.

5. Other Designated Contacts

- List other key personnel, if applicable; include their title, address, email address, and phone number.

6. Assignment of Security Responsibility

- Name, title, address, email address, and phone number of person who is responsible for the security of the system.

7. Information System Operational Status

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

8. Information System Type

- Indicate if the system is a major application or a general support system.

9. General System Description/Purpose

- Describe the function or purpose of the system and the information processes.

10. System Environment

- Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.

11. System Interconnections/Information Sharing

- List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, C&A status, and the name of the authorizing official.

12. Related Laws/Regulations/Policies

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

13. Minimum Security Controls

- Provide a thorough description of how the minimum controls in the applicable baseline are being implemented or planned to be implemented. The controls should be described by control family and indicate whether it is a system control, hybrid control, common control, scoping guidance is applied, or a compensating control is being used.

14. Information System Security Plan Completion Date

- Enter the completion date of the plan.

15. Information System Security Plan Approval Date

- Enter the date the system security plan was approved and indicate if the approval documentation is attached or on file.