NIST Special Publication 800-53A

Guide for Assessing the Security Controls in Federal Information Systems

Ron Ross
Arnold Johnson
Stu Katzke
Patricia Toth
George Rogers

I N F O R M A T I O N S E C U R I T Y

INITIAL PUBLIC DRAFT

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

July 2005

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

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

National Institute of Standards and Technology
Hratch G. Semerjian, Jr., Acting Director

Reports on Computer Systems Technology

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

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

National Institute of Standards and Technology Special Publication 800-53A, 152 pages

(July 2005) CODEN: NSPUE2

There are references in this publication to FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, currently under development by NIST in accordance with responsibilities assigned to NIST under the Federal Information Security Management Act of 2002. FIPS 200 will make the security controls defined in NIST Special Publication 800-53 mandatory for all federal information systems other than national security systems. The methodologies in this document may be used even before the completion of FIPS 200 in assessing the security controls in NIST Special Publication 800-53. For planning and transition purposes, agencies may wish to closely follow the development of FIPS 200 by NIST. Individuals are also encouraged to review the public drafts of the FISMA-related documents and offer their comments to NIST. All NIST publications other than the one noted above, are available at: http://csrc.nist.gov/publications.

THE PUBLIC COMMENT PERIOD FOR THIS DOCUMENT BEGINS ON JULY 15, 2005 AND ENDS ON AUGUST 31, 2005. COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, NIST, VIA ELECTRONIC MAIL AT SEC-CERT@NIST.GOV OR VIA REGULAR MAIL AT

100 BUREAU DRIVE (MAIL STOP 8930)
GAITHERSBURG, MD 20899-8930

Acknowledgements

The authors, Ron Ross, Arnold Johnson, Stu Katzke, Patricia Toth, and George Rogers wish to thank their colleagues who reviewed drafts of this document and contributed to its development. The authors also gratefully acknowledge and appreciate the many contributions from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Notes to Reviewers

NIST invites the public to review and comment upon this draft guideline. The initial public draft of Special Publication 800-53A contains assessment methods and procedures for the security controls in five of the seventeen security control families contained in Special Publication 800-53. We are interested in your feedback on:

- The conceptual assessment framework used to develop the assessment procedures;
- The individual assessment procedures in the master catalog (Appendix F);
- The recommended guidance on organizing and streamlining assessment procedures and reusing assessment results, where applicable, for security assessment plans; and
- The cost and potential impact on organizations in using the assessment methods and procedures to determine the effectiveness of security controls in organizational information systems.

Comments will be accepted through **August 31, 2005**. NIST will then revise the guideline and publish the final guideline with the remaining twelve families of assessment procedures by the end of 2005. Comments should be forwarded to the Computer Security Division, Information Technology Laboratory at NIST or submitted via email to sec-cert@nist.gov. The FISMA Implementation Project main website at http://csrc.nist.gov/sec-cert contains information on all of the FISMA-related security standards and guidelines and how the publications can be used to manage enterprise risk and build a comprehensive information security program.

Your feedback to us, as always, is critical in the security standards and guidelines development process to ensure that the work products produced by NIST are meeting the security needs of the federal government and the constituencies in the private sector who voluntarily use those products.

-- RON ROSS
PROJECT LEADER, FISMA IMPLEMENTATION PROJECT

Table of Contents

CHAPTER ONE

INTRODUCTION

THE NEED TO ASSESS SECURITY CONTROL EFFECTIVENESS IN INFORMATION SYSTEMS

The selection and employment of appropriate *security controls* for an information system[1] is an important task that can have major implications on the operations[2] and assets of an organization. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.[3] Once employed within an information system, security controls must be assessed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Security assessments play an important role in the information security programs of organizations. These assessments can be used to support a variety of security-related activities including but not limited to: (i) the testing and evaluation of security controls during the development of an information system; (ii) the information system security certification and accreditation process;[4] (iii) the annual testing and evaluation of security controls required by the Federal Information Security Management Act (FISMA); and (iv) generalized security reviews and audits. The results of security assessments contribute to the knowledge base of organizational officials with regard to the security status of the information system and the overall risk to the operations and assets of the organization incurred by the operation of the system.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for assessing the effectiveness of security controls employed in information systems supporting the executive agencies of the federal government. The guidelines apply to the security controls defined in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. The guidelines have been developed to help achieve more secure information systems within the federal government by:

- Enabling more consistent, comparable, and repeatable assessments of security controls;
- Facilitating more cost-effective assessments of security control effectiveness;
- Promoting a better understanding of the risks to organizational operations, organizational assets, or individuals resulting from the operation of information systems; and
- Creating more complete, reliable, and trustworthy information for organizational officials—to support security accreditation decisions and the annual FISMA reporting requirements.

[1] An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[2] Organizational operations include mission, functions, image, and reputation.

[3] Management controls are the safeguards or countermeasures that focus on the management of risk and the management of information system security. Operational controls are the safeguards or countermeasures that primarily are implemented and executed by people (as opposed to systems). Technical controls are the safeguards or countermeasures that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

[4] NIST Special Publication 800-37 provides guidance on security certification and accreditation of federal information systems.

The guidelines provided in this special publication are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.[5] The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems. In addition to the agencies of the federal government, state, local, and tribal governments, and private sector organizations that compose the critical infrastructure of the United States, are encouraged to consider the use of these guidelines, as appropriate.

Organizations should use NIST Special Publication 800-53A to create viable assessment plans to determine the effectiveness of the security controls employed within organizational information systems. The assessment methods and procedures from Special Publication 800-53A should be used as a starting point for and input to these assessment plans. Organizations should adjust and supplement the assessment procedures from this publication, taking into consideration platform-specific (i.e., hardware, software, or firmware) dependencies or organizational dependencies resulting from the employment of the security controls in the information system. The selection of appropriate assessment procedures for a particular organizational information system depends on three factors:

- The specific security controls selected and employed by the organization to protect the information system;
- The FIPS 199/Special Publication 800-53 impact level of the information system; and
- The assurance or level of confidence that the organization must have in determining the effectiveness of the security controls in the information system.

Risk assessments should be used to guide the rigor and intensity of all security control assessment-related activities associated with the information system to enable a cost-effective, risk-based implementation of this key element in the organization's information security program. The use of the assessment methods and procedures from Special Publication 800-53A as a starting point in the security control assessment process, promotes a more consistent level of security in organizational information systems. It also offers the needed flexibility to tailor the assessment methods and procedures based on specific organizational policy and requirements documents, particular conditions and circumstances, known threat and vulnerability information, or tolerance for risk to the organization's operations and assets.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse federal audience of information system and information security professionals including: (i) individuals with information system and information security management and oversight responsibilities (e.g., chief information officers, senior agency information security officers, and authorizing officials); (ii) individuals with information system development responsibilities (e.g., program and project managers); (iii) individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, information system security officers); and (iv) individuals with information system and information security assessment and monitoring responsibilities (e.g., auditors, inspectors general, evaluators, and certification agents). Commercial companies providing security control assessment, security certification, or auditing services can also benefit from the information in this publication.

[5] NIST Special Publication 800-59 provides guidance on identifying an information system as a national security system.

1.3 SYSTEM DEVELOPMENT LIFE CYCLE

Security assessments can be conducted at various phases in the System Development Life Cycle (SDLC).[6] For example, security assessments can be initiated during the system development and acquisition phase of the SDLC by information system developers or system integrators to ensure the security controls required for the protection of the system are properly designed, developed, and implemented.[7] This assessment process is sometimes referred to as developmental security testing and evaluation. Security assessments can also be conducted by information system owners, independent certification agents, or auditors during the operations and maintenance phase of the SDLC to ensure that the security controls are effective in the operational environment where the information system is deployed.[8] Special Publication 800-53A provides a set of assessment methods and procedures to support the assessment activities that may be required for an information system during any phase of the SDLC. The results obtained from the assessments will, in all likelihood, be used in different ways and for different purposes in creating effective assurance arguments that the information system has adequate security to protect the operations and assets of the organization.

1.4 RELATIONSHIP TO OTHER ASSESSMENT-RELATED PUBLICATIONS

NIST Special Publication 800-53A has been designed to be used with NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. In particular, the assessment methods and procedures contained in this publication and the recommendations for developing security assessment plans for organizational information systems directly support the security certification phase in the four-phase certification and accreditation process. The primary objective of the security certification phase is to determine if the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.

Since many of the security controls required to protect organizational information systems will use commercial off-the-shelf information technology products, organizations are encouraged, whenever possible, to take advantage of the assessment results and associated assessment-related documentation and evidence available from independent, third-party product evaluations and validations. Product evaluations and validations are routinely conducted today on cryptographic modules and general information technology products such as operating systems, database systems, firewalls, intrusion detection devices, web browsers, smart cards, biometrics devices, general purpose application components, network devices, and hardware platforms using national and international standards such as FIPS 140-2, *Security Requirements for Cryptographic*

[6] There are typically five phases in the system development life cycle of an information system: (i) system initiation; (ii) system development and acquisition; (iii) system implementation; (iv) system operations and maintenance; and (v) system disposal. NIST Special Publication 800-64 provides guidance on the security considerations in the information system development life cycle.

[7] Security assessments can also be conducted by the developers of commercial off-the-shelf information technology component products that are to be used in organizational information systems. These types of assessments can be conducted either by the product developer during the development process or by independent, third-party testing laboratories after the development process has been completed.

[8] Security assessors using the assessment methods and procedures from NIST Special Publication 800-53A should work closely with information system owners and authorizing officials to ensure that the methods and procedures selected for the assessment are appropriate for the information system being assessed. Generalized application of the assessment methods and procedures without careful consideration of the particular information system and its operational environment may be detrimental to the overall assessment process and produce misleading results.

Modules, and ISO/IEC 15408, *Common Criteria for Information Technology Security Evaluation*. Once the information system component product responsible for providing a particular security capability is identified and associated with a particular security control in NIST Special Publication 800-53, the evidence produced during a product evaluation and validation process can be used with other available assessment-related evidence obtained from the application of the assessment procedures in this publication to build an effective assurance argument that the security control is effective in its application.[9]

The reuse of credible/applicable security assessment reports from previously documented and accepted/approved assessments of the information system can also be considered in developing the necessary evidence for determining security control effectiveness. Applying previous assessment results to current assessments requires a thorough analysis of the current security control conditions to determine if any changes have occurred since the previous assessment and if the previous assessment results are applicable to the current assessment. For example, reusing previous assessment results that involved examining an organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance may be perfectly acceptable if there have not been any significant changes to any of the above documents.

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security control assessments including: (i) the conceptual framework for the development of specific assessment procedures for the security controls in NIST Special Publication 800-53; (ii) a description and definition of the components that compose the assessment framework; (iii) the process of generating assessment procedures using the assessment framework; and (iv) the structure and organization of the master catalog of assessment procedures produced from applying the assessment framework to the security controls in Special Publication 800-53.
- **Chapter Three** describes the process of assessing the security controls in organizational information systems including: (i) how organizations use assessment results to build effective assurance arguments for determining security control effectiveness; (ii) the development of effective security assessment plans; (iii) the conduct of security assessments and the roles and responsibilities of different organizational entities involved in the assessments; and (iv) the documentation and analysis of assessment results and how the assessment results are used to support organizational information security programs.
- **Supporting appendices** provide more detailed security control assessment-related information including: (i) general references (Appendix A); (ii) definitions and terms (Appendix B); (iii) acronyms (Appendix C); (iv) a description of assessment methods that can be employed by assessors to assess the security controls in organizational information systems (Appendix D); (v) the assessment expectations for low-impact, moderate-impact, and high-impact information systems (Appendix E); (vi) a master catalog of assessment procedures that can be used to develop effective information security plans for assessing the effectiveness of security controls (Appendix F); and (vii) a worked example for effective organization of assessment procedures (Appendix G).

[9] Organizations conducting assessments of information systems should work with component product vendors, product developers, information system developers, information systems integrators, and commercial testing laboratories to obtain the essential product-level assessment evidence and documentation necessary to support the assessment of the security controls in those information systems.

CHAPTER TWO

THE FUNDAMENTALS

BASIC CONCEPTS ASSOCIATED WITH SECURITY CONTROL ASSESSMENTS

This chapter presents the fundamental concepts associated with the assessment of security controls employed in organizational information systems including: (i) a conceptual framework for developing assessment procedures; (ii) the definitions of individual assessment framework components; (iii) the process employed to generate assessment procedures; and (iv) the organization of the assessment procedures into a master catalog.

2.1 FRAMEWORK FOR DEVELOPING ASSESSMENT PROCEDURES

A conceptual framework is used to describe the process of creating assessment procedures for security controls defined in NIST Special Publication 800-53.[10] There are three top-level components to the conceptual framework: (i) an input component; (ii) a processing component; and (iii) an output component. The input component consists of a unique identifier for the security control that is the subject of the assessment (e.g., CP-1, CP-4 (1)) and the FIPS 199/NIST Special Publication 800-53 impact level (i.e., low, moderate, or high) of the information system where the control is employed. The processing component identifies a specific set of assessment objects and assessment methods that are associated with the security control identified in the input component. The output component consists of an assessment procedure (i.e., a set of procedural statements) that can be used by an assessor to determine the effectiveness of the security control. Figure 1.1 illustrates the components of the conceptual framework used to develop assessment procedures for a particular security control.

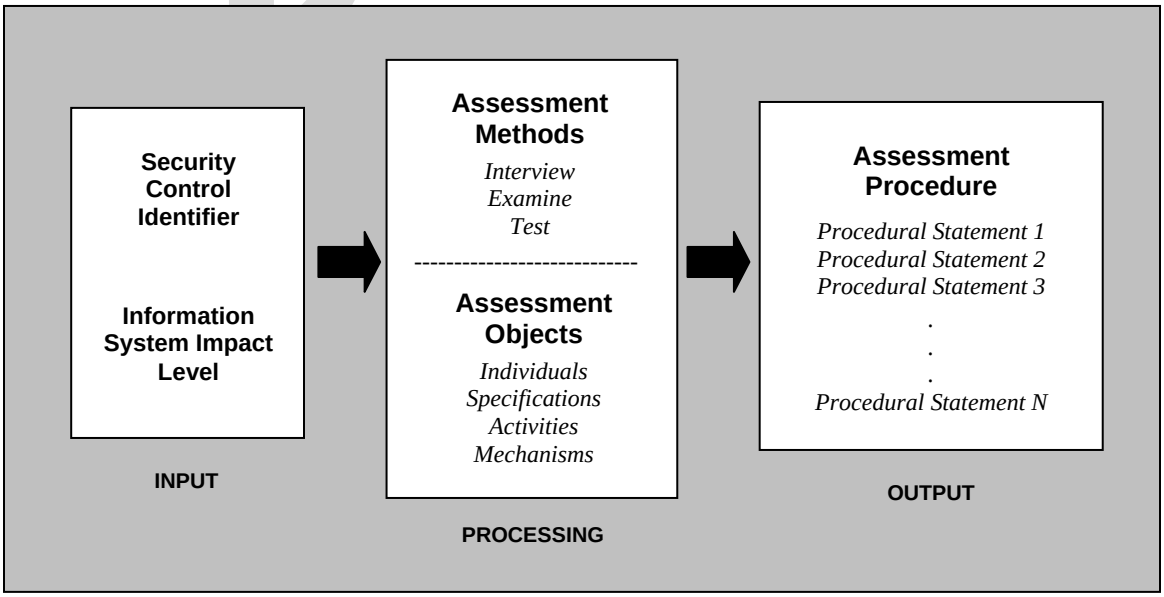

FIGURE 1.1 CONCEPTUAL FRAMEWORK FOR DEVELOPING ASSESSMENT PROCEDURES

[10] The conceptual framework has two primary objectives: (i) to show the technical basis and rationale for the procedural statements that are included in the assessment procedures generated for the security controls in NIST Special Publication 800-53; and (ii) to provide guidance for agencies in developing new or additional assessment procedures, when necessary.

2.2 DEFINING THE FRAMEWORK COMPONENTS

The assessment objects defined in the processing component of the framework include *specifications*, *mechanisms*, *activities*, and *individuals*. Specifications are the document-related artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system. Mechanisms are the specific protection-related items (e.g., hardware, software, firmware, or physical devices) employed within or at the boundary of an information system. Activities are the specific protection-related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic). Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above. With regard to the framework, each security control that is being assessed has a predefined set of assessment objects (e.g., specifications, mechanisms, activities, and individuals) associated with it.

The assessment methods defined in the processing component of the framework include *interview*, *examine*, and *test*. The interview method of assessment is the process of conducting focused discussions with individuals or groups of individuals within an organization to facilitate assessor understanding, achieve clarification, or obtain evidence. The examine method of assessment is the process of reviewing, checking, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities), and like the interview method, its primary purpose is to facilitate assessor understanding, achieve clarification, or obtain evidence. The test method of assessment is the process of exercising one or more assessment objects (limited to activities or mechanisms) under specified conditions to compare actual with expected behavior. In all three cases (i.e., interview, examine, and test) where the assessment methods are employed, the results are used to support the determination of overall security control effectiveness.

Each of the assessment methods described above has a set of associated attributes which help define the extent, rigor, and level of intensity of the assessment process. The three attributes employed within the conceptual framework are *scope*, *coverage*, and *depth*. The attributes are uniquely defined for each assessment method in the context of what the method is attempting to accomplish with regard to the production of evidence for the assessor. The depth attribute applies to both the interview and examine methods, the scope attribute applies only to the test method, and the coverage attribute applies to all three assessment methods. Attribute definitions and the complete description of each assessment method can be found in Appendix D.

In addition to the assessment method attributes, the assurance requirements defined in NIST Special Publication 800-53 play an important part in defining the extent, rigor, and level of intensity of security control assessments. The assurance requirements, levied on security control developers and implementers,[11] are associated with the three information system impact levels and security control baselines (i.e., low, moderate, high) described in NIST Special Publication 800-53. Based on the assurance requirements, the security control developers and implementers produce the necessary control documentation, conduct essential analyses, and define actions that must be performed during control operation to increase the level of confidence that the controls

[11] In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security controls for an information system. This may include, for example, hardware and software vendors providing the controls, contractors implementing the controls, or organizational personnel such as information system owners, information system security officers, system and network administrators, or other individuals with security responsibility for the information system.

are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Security control assessors subsequently use this information during the assessment process to develop the requisite evidence used to determine if security controls are effective in their application. To help assessors in determining the criteria for security control effectiveness, a set of assessment expectations is provided. The assessment expectations are associated with the assurance requirements in NIST Special Publication 800-53 and provide assessors with important reference points as to what results obtained from the application of the assessment procedures are acceptable for the determination of security control effectiveness. The assessment expectations for low-impact, moderate-impact, and high-impact information systems are provided in Appendix E.

2.3 GENERATING ASSESSMENT PROCEDURES

With respect to the components defined in the above framework, the generation of assessment procedures proceeds as follows. Using the unique identifier for the security control, the text of the control is parsed into assessable components. For example, consider the security control CP-1:

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

When parsing the control statement, the objects to be assessed are first identified. In this example, the control addresses both policy and procedures that, using the definitions for assessment objects, are considered specifications. It is also assumed that individuals are involved in the application of the policy and procedures. Thus, the assessment objects for the control are policy specifications, procedure specifications, and individuals. Next, the assessment methods to be used in assessing the objects are identified. In accordance with the assessment method descriptions in Appendix D, the examine method is used to make assessments based upon specifications and the interview method is used to make assessments based upon the knowledge of competent individuals. The control statement also defines what is expected to be achieved by applying the control within the information system. In this example, there are several required actions defined in the security control including developing, documenting, disseminating, and updating the contingency planning policy and procedures. In addition, the control requires the contingency planning policy to address purpose, scope, roles, responsibilities, and compliance, and requires procedures for implementing contingency planning policy and for each of the associated contingency planning controls.

Given the above decomposition, the selected assessment methods are applied to the appropriate assessment objects to produce a set of procedural statements that, taken together, comprise the overall assessment procedure for the security control. The individual procedural statements within the assessment procedure provide the necessary granularity to focus attention on the particular assessment methods and assessment objects required to determine security control effectiveness. A similar process occurs for the assurance requirements associated with a particular control. Thus, the assessment procedure for the security control CP-1, when employed in a low-impact information system, consists of the following procedural statements:

*CP-1.1. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine if contingency planning policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by*

responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required.

CP-1.2. ***Examine*** *the contingency planning policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, and compliance for contingency operations.*

CP-1.3. ***Examine*** *the contingency planning procedures to determine if the procedures are sufficient to address all areas identified in the contingency planning policy and all associated contingency planning controls.*

For a moderate-impact information system, the following procedural statements are added to the assessment procedure used to assess security control CP-1:

CP-1.4. ***Examine*** *the contingency planning policy and procedures to determine if the policy and procedures are updated periodically, when organizational reviews indicate updates are required.*

CP-1.5. ***Examine*** *the contingency planning policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance.*

CP-1.6. ***Examine*** *the contingency planning policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the policy and procedures are disseminated, periodically reviewed, and updated.*

And finally, the following procedural statements are added to the assessment procedure used to assess security control CP-1 in a high-impact information system:

CP-1.7. ***Interview*** *selected organizational personnel with contingency planning and plan implementation responsibilities and* ***examine*** *organizational records or documents to determine if anomalies or problems discovered by the organization in the content or application of the contingency planning policy and procedures are being documented and the resulting information used to actively improve the policy and procedures.*

CP-1.8. ***Interview*** *selected organizational personnel with contingency planning and plan implementation responsibilities and* ***examine*** *organizational records or documents to determine: (i) if the contingency planning policy and procedure dissemination, reviews, and updates are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the dissemination, reviews, and updates of the policy and procedures are being documented and the resulting information used to actively improve the dissemination, review, and update processes on a continuous basis.*

2.4 CATALOGING ASSESSMENT PROCEDURES

The discussion in the preceding sections illustrates the logical process of how assessment procedures are generated using the assessment framework. The framework ensures that the procedures used to assess the security controls in NIST Special Publication 800-53 are complete, consistent, and well-formed. Ultimately, the assessment procedures become part of a master catalog of procedures (Appendix F), which documents and organizes the procedures according to the seventeen families of security controls defined in Special Publication 800-53. Each assessment procedure in the catalog is composed of four parts: (i) a *security control* section; (ii) *an assessment methods* section; (iii) an *assessment objects* section; and (iv) an *assessment procedure* section. The security control section includes a two-character control identifier, the control name, and the control statement. The assessment methods section identifies the potential methods (i.e., interview, examine, and test) that are to be used in assessing the assessment objects

associated with the security control. The assessment objects section identifies the class of the objects of the assessment (i.e., specifications, mechanisms, activities and/or individuals). The assessment procedure section consists of a set of procedural statements, which are used in assessing some particular aspect of the security control (as described by the individual procedural statements). Each procedural statement contains a unique statement identifier followed by the procedural statement, and a notation as to the applicability of the procedural statement to the particular impact level of the information system where the security control is employed (i.e., low-impact, moderate-impact, or high-impact information system). There is also an optional category for applicability indicating that the security control is in the security control catalog, but is not included in any of the security control baselines defined in Special Publication 800-53. The following example illustrates a complete set of assessment procedures for the CP-5 security control from the contingency planning family in Special Publication 800-53.

CP-5 CONTINGENCY PLAN UPDATE

Control: The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*CP-5.1. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine if the contingency plan is updated in accordance with organization-defined frequency (at least annually).*

Applicability: All impact levels

*CP-5.2. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** records of information system/organizational changes or problems encountered during contingency plan implementation, execution, or testing to determine if needed changes are reflected in the contingency plan.*

Applicability: All impact levels

*CP-5.3. **Examine** the contingency plan to determine if the revised plan reflects the needed changes based on the organization's experiences during plan implementation, execution, and testing.*

Applicability: All impact levels

*CP-5.4. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that contingency plan reviews and updates for the information system are conducted correctly.*

Applicability: Moderate and High impact levels

*CP-5.5. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine: (i) if the contingency plan is being consistently reviewed and updated on an ongoing basis; and (ii) if anomalies or problems encountered during the plan update process are being documented and the resulting information used to actively improve the plan update policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Organizations can use the assessment procedures in the master catalog as a starting point for developing comprehensive security assessment plans to support a variety of potential assessment activities associated with determining the effectiveness of security controls in organizational information systems. Chapter Three provides guidance on developing effective security assessment plans using the assessment procedures from the master catalog of procedures in Appendix F.

CHAPTER THREE

THE PROCESS

CONDUCTING EFFECTIVE SECURITY ASSESSMENTS

This chapter describes the process of assessing the security controls in organizational information systems including: (i) considerations for building effective assurance arguments; (ii) the development of comprehensive security assessment plans to guide and inform assessment activities; (iii) the conduct of security assessments and the roles and responsibilities of key organizational elements; and (iv) the documentation and analysis of assessment results.

3.1 BUILDING EFFECTVE ASSURANCE ARGUMENTS

Today's information systems are incredibly complex assemblages of hardware, software and firmware components, all working together to provide organizations with the capability to process, store, and transmit information on a timely basis to support organizational missions and business cases. The protection of the underlying information systems that support those important missions and business cases is paramount to the success of the organization. Understanding the level of effectiveness of the security controls selected and implemented to provide the fundamental security capability for the information system is essential in determining the residual system vulnerabilities that, if exploited by threat agents, could adversely impact the operations (including mission, functions, image, or reputation) and assets of the organization.

Determining security control effectiveness is a complex process that involves building effective assurance arguments that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the information system. Assessors should gather as much evidence as possible during the assessment process to allow appropriate organizational officials to make credible, risk-based decisions on whether the security controls employed within the organization's information systems are effective in their application. The evidence needed to make such effective assurance arguments will, in most cases, be obtained from a variety of sources. The two principal sources of evidence for building effective assurance arguments come from product- and system-level assessments. Product-level assessments are typically conducted by independent, third-party testing organizations. Since many commercial products are assessed by the testing organization and then subsequently deployed in hundreds of thousands of information systems, the evaluations can, in many cases, be carried out at a greater level of depth and provide deeper insights into the security capabilities of the particular products.

System-level assessments are typically conducted by information systems developers, systems integrators, certification agents, auditors, information system owners, and the information security staffs of organizations. These assessors or assessment teams bring together the assessment results from product-level assessments, if available, and conduct additional system-level assessments using a variety of methods and techniques. The system-level assessments generate the necessary evidence to determine the overall effectiveness of the security controls employed in the organization's information systems and assurance that the manner in which the products have been integrated into those systems has not compromised the security of the products. Ultimately, organizations must determine how much evidence is needed to provide a sufficient level of confidence in the security controls that are protecting the organization's information systems.

3.2 DEVELOPING SECURITY ASSESSMENT PLANS

The *security assessment plan* provides the goals and objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. The output and end result of the security assessment is the *security assessment report*, which is one of three key components in the security accreditation package developed by information system owners for authorizing officials.[12] The security assessment report indicates the overall effectiveness of the security controls employed in the organizational information system and facilitates the determination of residual vulnerabilities in the system. The residual vulnerabilities are a key factor in the authorizing official's determination of risk to organizational operations (i.e., mission, functions, image, or reputation) or organizational assets.

The security control assessor is responsible for determining the effectiveness of the security controls in the organization's information system. The security control assessor is *not* responsible for determining if the organization has selected the appropriate set of security controls to achieve *adequate security* in protecting organizational operations and assets. The selection of the appropriate set of security controls for the information system is the responsibility of the information system owner and other organizational officials (e.g., Chief Information Officer, Senior Agency Information Security Officer, and Authorizing Official) in accordance with the organization's assessment of risk and other operational factors. Security control assessors should, however, point out prior to the actual assessment of the controls, any apparent discrepancies in the information system security plan in meeting the minimum security requirements defined in FIPS 200 and the minimum security control baselines established in NIST Special Publication 800-53.

Step 1: Establish which security controls are in scope for the assessment.

The security plan for the organizational information system undergoing assessment provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The assessor should use the controls described in the security plan to determine the scope of the assessment. Assessors should also note which security controls in the security plan are designated as common controls. The common controls may have been previously assessed as part of the organization's enterprise-wide information security program.[13] Assessors should coordinate the assessment of the information system with appropriate organizational officials (e.g., Chief Information Officer, Senior Agency Information Security Officer, Authorizing Official) to obtain the results of common security control assessments or (if the common security controls have not been assessed or are due to be reassessed) to make the necessary arrangements to include the common controls in the current assessment.

Step 2: Select the appropriate procedures to assess the security controls.

NIST Special Publication 800-53A provides an appropriate assessment procedure for each security control in NIST Special Publication 800-53. As a starting point, assessors should consider including in their assessment plans, the recommended assessment procedures for the set of security controls documented in the organization's security plan for the information system being assessed. For each security control in the security plan, assessors should review the

[12] In accordance with NIST Special Publication 800-37, the security accreditation package consists of the security plan, the security assessment report, and the plan of action and milestones.

[13] NIST Special Publications 800-37 and 800-53 provide guidance on the employment and use of common security controls in organizational information systems.

corresponding assessment procedure in Appendix F. Based on the impact level of the information system as defined in FIPS 199 and NIST Special Publication 800-53, assessors can select the appropriate procedural steps within the assessment procedure that apply to that impact level. The number of procedural steps increases with the impact level of the information system representing a greater rigor in and intensity of the assessment process. In addition, during the tailoring of the initial security control baseline in accordance with the process described in NIST Special Publication 800-53, selected security controls may have been eliminated or downgraded, or the organization may have employed compensating controls. The selection of appropriate procedural steps should be adjusted accordingly.

Step 3: Optimize the selected assessment procedures to ensure maximum efficiency.

During the assessment of an organizational information system, assessment methods are applied numerous times to a variety of assessment objects within a particular family of security controls. To save time and reduce assessment costs, assessors should review the selected assessment procedures for the security control family and combine/consolidate procedural steps whenever possible or practicable. For example, assessors may wish to consolidate interviews for key organizational officials dealing with contingency planning operations. Appendix G provides a detailed example of the type of assessment procedure organization that can be applied by assessors in constructing an efficient assessment plan for the information system. Additional efficiencies may be realized by assessing potential optimizations across the seventeen security control families in Special Publication 800-53; however, those optimizations are beyond the scope of this publication.

Step 4: Develop additional assessment procedures, if needed.

Based on an assessment of risk, organizations may choose to develop and implement additional security controls for their information systems that are beyond the scope of NIST Special Publication 800-53. In these situations, assessors should use the assessment framework described in Chapter Two to develop assessment procedures for those security controls. The additional assessment procedures should be integrated into the security assessment plan. In addition to the development of assessment procedures, the procedures in NIST Special Publication 800-53A may be extended or adapted to address platform-specific or organization-specific dependencies. This situation arises most often in the assessment procedures associated with the security controls from the technical families in NIST Special Publication 800-53. Platform-specific assessment procedures are beyond the scope of this publication.

Step 5: Obtain assessment results from previous security control assessments.

Assessors should take advantage of assessment results and assessment evidence generated during previous security control assessments. Depending on the length of time since the previous assessment and the level of depth/rigor of the assessment process, assessors may gain significant insights into the state of the security controls in the information system by considering such previously generated assessment results and evidence. This information may be extremely useful in helping to determine the effectiveness of the current set of security controls employed by the organization and may be effectively incorporated into the security assessment plan. The use and acceptability of previous assessment results and assessment evidence in the security assessment plan should be coordinated with and approved by the information system owner in collaboration with appropriate organizational officials (e.g., Chief Information Officer, Senior Agency Information Security Officer, Authorizing Official) and should not conflict with federal legislation, policies, directives, standards, or guidelines with respect to the assessment of security controls.

Step 6: Finalize the security assessment plan and obtain approval to execute the plan.

After the assessment procedures are selected (or developed for those procedures not contained in the catalog of procedures), organized for efficiency, extended/adapted for platform or organizational dependencies, and supplemented with additional information from previous assessments, the assessment schedule is established along with key milestones for the assessment process. Once the security assessment plan is completed, the plan should be reviewed and approved by appropriate organizational officials to ensure that the plan is complete, consistent with the security objectives of the organization, and cost-effective with regard to the resources allocated for the assessment.[14]

3.3 DOCUMENTING AND ANALYZING ASSESSMENT RESULTS

After the security assessment plan is completed and approved by the organization, the security assessment is initiated by the assessor or security assessment team.[15] The assessor or assessment team executes the security assessment plan in accordance with the agreed-upon milestones and schedule. The assessment results should be fully documented in accordance with the reporting format described in NIST Special Publication 800-26, *Guide for Information Security Program Assessment and System Reporting Form* (initial public draft, July 2005).[16] The reporting format provided in Special Publication 800-26 can be used for any type of security assessment including self-assessments by information system owners, independent third-party assessments by certification agents supporting a security accreditation process, or independent audits of security controls by auditors or inspectors general. Once the results of the security assessment are documented, the analysis of the data collected can begin.

Applying the designated assessment methods and associated procedural statements to selected assessment objects produces results that are used to determine the overall effectiveness of a particular security control (i.e., is the control implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system?). However, the determination of security control effectiveness is not always straightforward and can be somewhat subjective in nature. This situation arises because each procedural statement contained within an assessment procedure executed by the assessor can result in a determination of: (i) *fully satisfied*; (ii) *partially satisfied*; or (iii) *not satisfied*. Fully satisfied indicates that the portion of the security control being addressed by the procedural statement has produced a fully acceptable result. Partially satisfied indicates that the portion of the security control being addressed by the procedural statement has produced a partially, but not fully acceptable result. Not satisfied indicates that the portion of the security control being addressed by the procedural statement has produced an unacceptable result. When the execution of a procedural statement results in a partially satisfied or not satisfied condition, assessors should indicate which portions of the security control have not be implemented or applied.

There are no strict rules for determining overall security control effectiveness. In general, for a security control to be deemed effective in its application, there must be a preponderance of

[14] For self-assessments, the security plan approval step can be omitted.

[15] The size and organizational makeup of the security assessment team (i.e., skill sets, technical expertise, and assessment experience of the individuals composing the team) is at the discretion of the organization requesting and initiating the assessment of the information system.

[16] Special Publication 800-26, formerly known as the *Security Self-Assessment Guide for Information Technology Systems*, has been reengineered and updated to conform to the new FISMA-related security standards and guidelines being developed by NIST. The revised publication will serve as the principal reporting mechanism for organizations conducting security assessments on the security controls employed within their information systems.

supporting evidence that all aspects of the security control have been addressed and that the control meets its intended function or purpose. Assessors should identify and document any vulnerabilities introduced into the information system by a partial or complete failure of individual or groups of security controls. This information is used as the organization's primary input to the plan of action and milestones for the information system and provides a detailed roadmap for addressing/correcting the noted deficiencies in the security controls. Authorizing officials, in consultation and collaboration with their security staffs, use the assessment results and the information produced on residual vulnerabilities in the information system, to determine the overall risk to organizational operations and assets by placing the system into operation or continuing its operation.

3.4 CONTINUOUS MONITORING

Conducting a thorough assessment of the security controls in an organizational information system is a necessary but not sufficient condition to demonstrate security due diligence. Effective information security programs should also include an aggressive continuous monitoring program to check the status of the security controls in the information system on an ongoing basis. Continuous monitoring, the fourth phase in the security certification and accreditation process, is a proven technique to address the security impacts in information systems resulting from changes to the hardware, software, or firmware. An effective continuous monitoring program requires:

- Configuration management and control processes for the information system;
- Security impact analyses on changes to the information system; and
- Assessment of selected security controls in the information system and security status reporting to appropriate agency officials.[17]

With regard to configuration management and control, it is important to document the proposed or actual changes to the information system and to subsequently determine the impact of those proposed or actual changes on the security of the system. Information systems will typically be in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the surrounding environment where the system resides. Documenting information system changes and assessing the potential impact those changes may have on the security of the system is an essential aspect of continuous monitoring and maintaining the security accreditation. The results of continuous monitoring should be reported to the authorizing official and senior agency information security officer on a regular basis. The continuous monitoring results should also be considered with respect to any necessary updates to the information system security plan and to the plan of action and milestones, since the authorizing official, senior agency information security officer, information system owner, and security assessor will be using these plans to guide future security assessment activities.

[17] At the discretion of the agency, the security status reports on agency information systems can be used to help satisfy the FISMA reporting requirement for documenting remedial actions for any security-related deficiencies.

APPENDIX A

REFERENCES

LAWS, DIRECTIVES, POLICIES, STANDARDS, AND GUIDELINES[18]

1. Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, May 2003.
2. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protective Distribution Systems (PDS)*, December 1996.
3. Department of Defense Instruction 8500.2, *Information Assurance Implementation*, February 2003.
4. Department of Health and Human Services Centers for Medicare and Medicaid Services (CMS), *Core Set of Security Requirements*, February 2004.
5. Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*, May 2000.
6. Director of Central Intelligence Directive 6/3 Policy, *Protecting Sensitive Compartmented Information within Information Systems*, June 1999.
7. Electronic Government Act (P.L. 107-347), December 2002.
8. Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
9. Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* (projected for publication December 2005).
10. Federal Information Processing Standards Publication 201, *Personal Identity Verification for Federal Employees and Contractors*, February 2005.
11. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
12. General Accounting Office *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6, January 1999.
13. Information Technology Management Reform Act (P.L. 104-106), August 1996.
14. International Organization for Standardization/International Electrotechnical Commission FDIS 17799, *Code of Practice for Information Security Management*, November 2004.
15. National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.
16. National Institute of Standards and Technology Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, (Initial public draft, July 2005).

[18] The status and most current versions of NIST publications to include FIPS and Special Publications in the 800-series (draft and final) can be found at http://csrc.nist.gov/publications.

17. National Institute of Standards and Technology Special Publication 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.

18. National Institute of Standards and Technology Special Publication 800-26, *Guide for Information Security Program Assessment and System Reporting Form*, (Initial public draft, July 2005).

19. National Institute of Standards and Technology Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, Revision A, June 2004.

20. National Institute of Standards and Technology Special Publication 800-28, *Guidelines on Active Content and Mobile Code*, October 2001.

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

22. National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

23. National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

24. National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting Information Security Products*, October 2003.

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

26. National Institute of Standards and Technology Special Publication 800-40, *Procedures for Handling Security Patches*, August 2002.

27. National Institute of Standards and Technology Special Publication 800-42, *Guideline on Network Security Testing*, October 2003.

28. National Institute of Standards and Technology Special Publication 800-45, *Guidelines on Electronic Mail Security*, September 2002.

29. National Institute of Standards and Technology Special Publication 800-46, *Security for Telecommuting and Broadband Communications*, August 2002.

30. National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

31. National Institute of Standards and Technology Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002.

32. National Institute of Standards and Technology Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.

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

34. National Institute of Standards and Technology Special Publication 800-56, *Recommendation on Key Establishment Schemes*, (initial public draft) January 2003.

35. National Institute of Standards and Technology Special Publication 800-57, *Recommendation for Key Management*, (draft) April 2005.

36. National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, January 2005.

37. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

38. National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

39. National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2004.

40. National Institute of Standards and Technology Special Publication 800-63, Version 1.0.1, *Electronic Authentication Guideline*, September 2004.

41. National Institute of Standards and Technology Special Publication 800-64, Revision1, *Security Considerations in the Information System Development Life Cycle*, June 2004.

42. National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.

43. National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, May 2005.

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

45. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *Business Reference Model* (v2.0), June 2003.

46. Office of Management and Budget Memorandum 03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 2003.

47. Office of Management and Budget Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003.

48. Office of Management and Budget Memorandum 04-04, *E-Authentication Guidance for Federal Agencies*, December 2003.

49. Paperwork Reduction Act of 1995 (P.L. 104-13), May 1995.

50. Privacy Act of 1974 (P.L. 93-579), September 1975.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-53A. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Accreditation [NIST SP 800-37]	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Accreditation Boundary [NIST SP 800-37]	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.
Accrediting Authority	See Authorizing Official.
Activities	An assessment object that includes specific protection-related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic).
Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Agency	See Executive Agency.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.
Authorize Processing	See Accreditation.
Authorizing Official [NIST SP 800-37]	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.

Certification [NIST SP 800-37]	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Certification Agent [NIST SP 800-37]	The individual, group, or organization responsible for conducting a security certification.
Chief Information Officer [44 U.S.C., Sec. 5125(b)]	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Common Security Control [NIST SP 800-37]	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control [CNSS Inst. 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications before, during, and after system implementation.
Countermeasures [CNSS Inst. 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

Controlled Interface [CNSS Inst. 4009]	Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
Federal Enterprise Architecture [FEA Program Management Office]	A business-based framework for government wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
General Support System [OMB Circular A-130, Appendix III]	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.
Individuals	An assessment object that includes people applying specifications, mechanisms, or activities.
High-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
Information Owner [CNSS Inst. 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy [CNSS Inst. 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information System [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner (or Program Manager) [CNSS Inst. 4009, Adapted]	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information System Security Officer [CNSS Inst. 4009, Adapted]	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program.
Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, executive order, directive, policy, or regulation.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Label	See Security Label.
Low-Impact System	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
Major Application [OMB Circular A-130, Appendix III]	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.
Major Information System [OMB Circular A-130]	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

Management Controls [NIST SP 800-18]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Mechanisms	An assessment object that includes specific protection-related items (e.g., hardware, software, firmware, or physical devices) employed within or at the boundary of an information system.
Media Access Control Address	A hardware address that uniquely identifies each component of an IEEE 802-based network. On networks that do not conform to the IEEE 802 standards but do conform to the OSI Reference Model, the node address is called the Data Link Control (DLC) address.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).
Moderate-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate, and no security objective is assigned a FIPS 199 potential impact value of high.
National Security Emergency Preparedness Telecommunications Services [47 C.F.R., Part 64, App A]	Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Non-repudiation [CNSS Inst. 4009]	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Operational Controls [NIST SP 800-18]	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Privacy Impact Assessment [OMB Memorandum 03-22]	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Protective Distribution System	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.

Records	The recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Remote Access	Access by users (or information systems) communicating external to an information system security perimeter.
Remote Maintenance	Maintenance activities conducted by individuals communicating external to an information system security perimeter.
Risk [NIST SP 800-30]	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals results from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment [NIST SP 800-30]	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Risk Management [NIST SP 800-30]	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
Safeguards [CNSS Inst. 4009, Adapted]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Sanitization [CNSS Inst. 4009, Adapted]	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
Scoping Guidance	Provides organizations with specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations on the applicability and implementation of individual security controls in the control baseline.

Security Category [FIPS 199]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Baseline	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.
Security Impact Analysis [NIST SP 800-37]	The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.
Security Label	Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.
Security Objective	Confidentiality, integrity, or availability.
Security Perimeter	See Accreditation Boundary.
Security Plan	See System Security Plan.
Security Requirements	Requirements levied on an information system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.
Specifications	An assessment object that includes document-related artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge.

Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
System	See Information System.
System-specific Security Control [NIST SP 800-37]	A security control for an information system that has not been designated as a common security control.
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Technical Controls [NIST SP 800-18]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Threat [CNSS Inst. 4009, Adapted]	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Agent/Source [NIST SP 800-30]	Either: (i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability.
Threat Assessment [CNSS Inst. 4009]	Formal description and evaluation of threat to an information system.
Trusted Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by software that is not trusted.
User [CNSS Inst. 4009]	Individual or (system) process authorized to access an information system.
Vulnerability [CNSS Inst. 4009, Adapted]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment [CNSS Inst. 4009]	Formal description and evaluation of the vulnerabilities in an information system.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CNSS	Committee for National Security Systems
COTS	Commercial Off-The-Shelf
DCID	Director of Central Intelligence Directive
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standard(s)
FISMA	Federal Information Security Management Act
GOTS	Government Off-The-Shelf
IEEE	Institute of Electrical and Electronics Engineers
IPv6	Internet Protocol Version 6
MAC	Media Access Control
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
TCP/IP	Transmission Control Protocol/Internet Protocol
USC	United States Code
VPN	Virtual Private Network
VOIP	Voice Over Internet Protocol

APPENDIX D

ASSESSMENT METHOD DESCRIPTIONS

ASSESSMENT METHOD DEFINITIONS, APPLICABLE OBJECTS, AND ATTRIBUTES

There are three assessment methods that can be used to help determine whether a particular security control employed within an information system is effective in its application: (i) interview; (ii) examine; and (iii) test. The information (or assessment evidence) obtained during the application of these assessment methods is used to determine the extent to which the security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Complete descriptions of the three assessment methods are provided below.

ASSESSMENT METHOD: Interview

DEFINITION: The process of conducting focused discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness.

ASSESSMENT OBJECTS: Individuals or groups of individuals

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include interviewing chief information officers, senior agency information security officers, authorizing officials, authorizing officials designated representatives, information owners, information system owners, information system security officers, information system security managers, personnel officers, human resource managers, facilities managers, training officers, information system operators, network and system administrators, site managers, physical security officers, and users.

ATTRIBUTES: Depth, Coverage

- The *depth* attribute addresses the rigor of and level of detail in the interview process. There are three possible values for the depth attribute: (i) abbreviated; (ii) substantial; and (iii) comprehensive.
  - *Abbreviated* interviews are informal, ad hoc interviews that consist of generalized, high-level discussions with selected organizational personnel on particular topics relating to the specifications, mechanisms, or activities associated with the security control being assessed (including the results of other assessment methods). This type of interviews is typically conducted using a set of generalized, high-level questions.
  - *Substantial* interviews are informal, structured interviews that consist of generalized, high-level discussions and specific discussions in targeted areas with selected organizational personnel on particular topics relating to the specifications, mechanisms, or activities associated with the security control being assessed (including the results of other assessment methods). This type of interview is typically conducted using a set of generalized, high-level questions and a set of more detailed questions in specific areas where assessment evidence allows or responses indicate a need for more detailed investigation.
  - *Comprehensive* interviews are formal, structured interviews that consist of generalized, high-level discussions and specific, in depth discussions with selected organizational personnel on particular topics relating to the specifications, mechanisms, or activities associated with the security control being assessed (including the results of other assessment methods). This type of interview is typically conducted using a set of generalized, high-level questions and a set of in depth, probing questions in all significant areas covered by the assessment.
- The *coverage* attribute addresses the types of individuals to be interviewed (by organizational roles and associated responsibilities) and the number of individuals to be interviewed (by type). Organizations, in collaboration with information system assessors, determine the specific types and numbers of individuals to be interviewed during the assessment process.

ASSESSMENT METHOD: Examine

DEFINITION: The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness.

ASSESSMENT OBJECTS: Specifications (e.g., policies, plans, procedures, system requirements, designs)
Mechanisms (e.g., hardware, software, firmware, physical devices)
Activities (e.g., system operations/administration/management, exercises, drills)

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include, for example: reviewing information security policies, plans, and procedures; analyzing system design documentation and interface specifications; observing system backup operations, reviewing and analyzing the results of contingency plan exercises or drills; observing incident response operations or activities; checking security configuration settings; or studying technical manuals and user/administrator guides. Applying the examine method to a particular security control may require examining multiple assessment objects of different types. The number and types of assessment objects examined is a function of the particular control, specifically its composition, design, and implementation. During the process of examining assessment objects, certain artifacts associated with those objects (e.g., records, logs, reports, test/evaluation/audit results) may also be assessed. To reduce the level of effort in examining assessment objects, assessors should, to the maximum extent possible, reuse examination results and evidence from previous security control assessments (when such results are available, there have been no substantial intervening changes to the information system that could invalidate the results, and they are judged to be credible).

ATTRIBUTES: Depth, Coverage

- The *depth* attribute addresses the rigor of and level of detail in the examination process. There are three possible values for the depth attribute: (i) abbreviated; (ii) substantial; and (iii) comprehensive.
  - *Abbreviated* examinations are examinations that consist of brief, high-level reviews, observations, or inspections of selected specifications, mechanisms, or activities associated with the security control being assessed using a limited body of evidence or documentation. These types of examinations are typically conducted using only functional-level descriptions of specifications, mechanisms, or activities, and employ checklists or other similar assessment techniques consistent with an abbreviated assessment period.
  - *Substantial* examinations are examinations that consist of detailed analyses, observations, or studies of selected specifications, mechanisms, or activities associated with the security control being assessed using a body of evidence or documentation that is greater than that available during abbreviated examinations. These types of examinations are typically conducted using functional-level descriptions of specifications, mechanisms, or activities, and where appropriate, high-level design information. Substantial examinations employ a variety of analysis techniques and require a longer assessment period than assessment periods for abbreviated examinations.
  - *Comprehensive* examinations are examinations that consist of detailed and thorough analyses, observations, or studies of selected specifications, mechanisms, or activities associated with the security control being assessed using a body of evidence or documentation that is greater than that available during substantial examinations. These types of examinations are typically conducted using functional-level descriptions of specifications, mechanisms, or activities, and where appropriate, high-level design, low-level design, and implementation-related information (e.g., source code). Comprehensive examinations employ a variety of sophisticated analysis techniques and require a longer assessment period than assessment periods for substantial examinations.
- The *coverage* attribute addresses the types of specifications, mechanisms, or activities to be examined and the number of specifications, mechanisms, or activities to be examined (by type). Organizations, in collaboration with information system assessors, determine the specific types and numbers of specifications, mechanisms, or activities to be assessed during the assessment process.

ASSESSMENT METHOD: Test

DEFINITION: The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness.[19]

ASSESSMENT OBJECTS: Mechanisms (e.g., hardware, software, firmware, physical devices)
Activities (e.g., system operations/administration/management, exercises, drills)

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include, for example: structural testing of the logical access control and encryption mechanisms; functional testing of the identification/authentication and audit mechanisms; functional testing of the security configuration settings; functional testing of the physical access control devices; penetration testing of the information system and its key components; functional testing of the information system backup operations; and functional testing of the incident response/contingency planning capability.[20] Applying the test method to a particular security control may require testing multiple assessment objects of different types. The number and types of assessment objects tested is a function of the particular control, specifically its composition, design, and implementation. During the process of testing assessment objects, certain artifacts associated with those objects (e.g., records, logs, reports, test/evaluation/audit results) may also be assessed. To reduce the level of effort in testing assessment objects, the assessor should, to the maximum extent possible, reuse test results and evidence from previous security control assessments (when such results are available, there have been no substantial intervening changes to the information system that could invalidate the results, and they are judged to be credible).

ATTRIBUTES: Scope, Coverage

- The *scope* attribute addresses the types of testing to be conducted. There are three possible values for the scope attribute: (i) functional testing; (ii) structural testing; and (iii) penetration testing.
  - *Functional* testing (i.e., black-box testing) is a test methodology that assumes knowledge of the functional specifications, high-level design, and operating specifications of the item under assessment.
  - *Structural* testing (i.e., gray-box, white-box testing) is a test methodology that assumes (some) explicit knowledge of the internal structure of the item under assessment (e.g., low-level design, source code implementation representation).
  - *Penetration* testing is a test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under no constraints, attempt to circumvent the security features of an information system.
- The *coverage* attribute addresses the types of mechanisms or activities to be tested and the number of mechanisms or activities to be tested (by type). Organizations, in collaboration with information system assessors, determine the specific types and numbers of mechanisms or activities to be assessed during the assessment process. For mechanism-related testing that involves software, the coverage attribute also addresses the extent of the testing conducted (e.g., number of test cases, number of modules tested, etc.).

[19] Testing is typically used to determine if assessment objects (i.e., mechanisms or activities) meet a set of pre-defined specifications. Testing can also include controlled demonstrations of specific mechanisms or activities by individuals or groups of individuals within the organization to provide assessors with evidence of security control effectiveness. Penetration testing is typically conducted only on mechanisms or groups of mechanisms employed within information systems.

[20] The type of testing noted in each of the examples does not take into account the impact level of the information system. Figure D-1 lists the actual types of testing to be conducted in accordance with information system impact levels.

Figure D-1 provides a summary of the assessment method attributes and attribute values by information system impact level.

ASSESSMENT METHODS: Interview, Examine, Test		**INFORMATION SYSTEM IMPACT LEVEL**		
ATTRIBUTE	**VALUE**	**LOW**	**MODERATE**	**HIGH**
Depth (Interview and examine methods only)	Abbreviated	√	---	---
	Substantial	---	√	---
	Comprehensive	---	---	√
Scope (Test method only)	Functional (black-box)	√	√	√
	Penetration	---	√	√
	Structural (gray-box, white-box)	---	---	√
Coverage (All methods)	Number and types of assessment objects determined by organizations in collaboration with assessors.[21]	√	√	√

FIGURE D-1: ASSESSMENT METHOD ATTRIBUTES AND ATTRIBUTE VALUES BY IMPACT LEVEL

[21] The types and numbers of assessment objects included in the assessment should be a function of the FIPS 199 and NIST Special Publication 800-53 impact level of the information system. Organizations should consider increasing the types and number of objects assessed as the impact level of the information system increases. The increased coverage, depth, and scope of an assessment, contributes to greater assurance in the overall effectiveness of the security control being assessed.

APPENDIX E

ASSESSMENT EXPECTATIONS

CHARACTERIZING THE EXPECTATIONS OF SECURITY ASSESSMENTS BY IMPACT LEVEL

The following sections establish the expectations for security control assessments based on the assurance requirements defined in NIST Special Publication 800-53. The assessment expectations provide assessors with important reference points as to what results obtained from the application of the assessment procedures are acceptable for the determination of security control effectiveness.

LOW-IMPACT INFORMATION SYSTEMS

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement.

Supplemental Guidance: For security controls in the low baseline, the focus is on the control being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.

Assessment Expectations: Abbreviated interviews and examinations are conducted. Functional testing is employed to ensure that there are no obvious errors in the security control.

For *specifications:*

- The assessor determines if the specification exists and is implemented within the organization.
- The assessor determines if the specification is consistent with the functional requirements in the security control statement.

For *mechanisms*:

- The assessor determines if the mechanism exists and is operational within the information system.
- The assessor determines if the mechanism is consistent with the functional requirements in the security control statement.

For *activities*:

- The assessor determines if the activity is being performed within the organization.
- The assessor determines if the activity is consistent with the functional requirements in the security control statement.

MODERATE-IMPACT INFORMATION SYSTEMS

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. **The control developer/implementer provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions to ensure that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.**

Supplemental Guidance: For security controls in the moderate baseline, the focus is on ensuring correct implementation and operation of the control. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities and produces specific documentation to ensure the control meets its required function or purpose.

Assessment Expectations: Substantial interviews and examinations are conducted. Functional and penetration testing are employed to ensure that there are no obvious errors in the security control and that the security control is implemented correctly and operating as intended.

For *specifications:*

- The assessor determines if the specification exists, is implemented within the organization, **and is unambiguous**.
- The assessor determines if the specification is consistent with the functional requirements in the security control statement.
- **The assessor determines if the specification includes an assignment of responsibilities and specific actions to ensure the specification is being applied/followed and meets its required function or purpose.**

For *mechanisms*:

- The assessor determines if the mechanism exists and is operational within the information system.
- The assessor determines if the mechanism is consistent with the functional requirements in the security control statement.
- **The assessor determines if the mechanism is implemented correctly (including installation) and operating as intended in accordance with developer/implementer specifications and defined procedures.**
- **The assessor determines if the mechanism includes an assignment of responsibilities and specific actions to ensure the mechanism is being employed and meets its required function or purpose.**

For *activities*:

- The assessor determines if the activity is being performed within the organization.
- The assessor determines if the activity is consistent with the functional requirements in the security control statement.
- **The assessor determines if the activity is being performed correctly in accordance with defined procedures.**
- **The assessor determines if the activity includes an assignment of responsibilities and specific actions to ensure the activity is being performed and meets its required function or purpose.**

HIGH-IMPACT INFORMATION SYSTEMS

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties **and design/implementation** of the control with sufficient detail to permit analysis and testing of the control (**including functional interfaces among control components)**. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions to ensure that when the control is implemented, it will **continuously and consistently (i.e., across the information system)** meet its required function or purpose **and support improvement in the effectiveness of the control**. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in the high baseline, the focus is expanded to require, within the control, the capabilities that are needed to support ongoing consistent operation of the control and continuous improvement in the control's effectiveness. The developer/implementer is expected to expend significant effort on the design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation to support these activities. For security controls in the high baseline, this same documentation is needed by assessors to analyze and test the internal components of the control as part of the overall assessment of the control.

Assessment Expectations: Comprehensive interviews and examinations are conducted. Functional, structural, and penetration testing are employed to ensure that there are no obvious errors in the security control, that the security control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is continuous improvement in security control effectiveness.

For *specifications:*

- The assessor determines if the specification exists, is implemented within the organization, and is unambiguous.
- The assessor determines if the specification is consistent with the functional requirements in the security control statement.
- The assessor determines if the specification includes an assignment of responsibilities and specific actions to ensure the specification is being applied/followed and meets its required function or purpose **consistently on an ongoing basis**.
- **The assessor determines if the specification includes a means to support the continuous improvement in its effectiveness.**

For *mechanisms*:

- The assessor determines if the mechanism exists and is operational within the information system.
- The assessor determines if the mechanism is consistent with the functional requirements in the security control statement.
- The assessor determines if the mechanism is implemented correctly (including installation) and operating as intended in accordance with developer/implementer specifications and defined procedures.
- The assessor determines if the mechanism includes an assignment of responsibilities and specific actions to ensure the mechanism is being effectively employed and meets its required function or purpose **consistently on an ongoing basis**.
- **The assessor determines if the mechanism includes a means to support the continuous improvement in its effectiveness.**

For *activities*:

- The assessor determines if the activity is being performed within the organization.
- The assessor determines if the activity is consistent with the functional requirements in the security control statement.
- The assessor determines if the activity is being performed correctly in accordance with defined procedures.
- The assessor determines if the activity includes an assignment of responsibilities and specific actions to ensure the activity is being performed and meets its required function or purpose **consistently on an ongoing basis**.
- **The assessor determines if the activity includes a means to support the continuous improvement in its effectiveness.**

Figure E-1 provides a summary of the assurance requirements for low-impact, moderate-impact, and high impact information systems.

ASSURANCE REQUIREMENTS	INFORMATION SYSTEM IMPACT LEVEL		
	LOW	MODERATE	HIGH
Security controls in place; no obvious errors	√	√	√
Security controls correctly implemented; operating as intended	---	√	√
Security controls consistently applied on an ongoing basis with continuous improvement	---	---	√

FIGURE E-1: ASSURANCE REQUIREMENTS BY INFORMATION SYSTEM IMPACT LEVEL

APPENDIX F

ASSESSMENT PROCEDURE CATALOG

METHODS, OBJECTS, AND PROCEDURES FOR ASSESSING SECURITY CONTROLS

This appendix provides an assessment procedure for each security control identified in the catalog of security controls in NIST Special Publication 800-53. The security control procedures are organized by security control families similar to that of the security control catalog in Special Publication 800-53. Each assessment procedure is composed of four parts: (i) a *security control* section; (ii) *an assessment methods* section; (iii) an *assessment objects* section; and (iv) an *assessment procedure* section. The security control section includes a two-character control identifier, the control name, and the control statement. The assessment methods section identifies the potential methods (i. e., interview, examine, and test) that are the subjects of the assessment to be used in assessing the assessment objects associated with the security control. The assessment objects section identifies the class of objects to be assessed (i. e., individuals,[22] specifications, mechanisms, and/or activities). The assessment procedure section consists of a set of procedural statements, which are used in assessing some particular aspect of the security control (as described by the individual procedural statements). Each procedural statement contains a unique statement identifier followed by the procedural statement, and a notation as to the applicability of the procedural statement to the particular impact level of the information system where the security control is employed (i.e., low-impact, moderate-impact, or high-impact information system). There is also an optional category for applicability indicating that the security control is in the security control catalog, but is not included in any of the security control baselines defined in Special Publication 800-53.

Each procedural statement identifies the assessment method to be used in the assessment of the security control, but does not directly reflect the appropriate extent, rigor, and level of intensity of the assessment process as defined by the attributes (e.g., depth, coverage, or scope) associated with each assessment method described in Appendix A. The attribute values assigned to the attributes associated with the assessment methods are a function of the impact level of the information system where the security control is employed. Therefore, when employing a particular assessment method in a procedural statement, the extent, rigor, and level of intensity applied during the assessment process should be guided by and consistent with the appropriate attribute values assigned to the attributes for the assessment method. See Appendix D and Figure D-1 for guidance on the application of the test method attributes.

[22] While the term *individual is* listed as class of assessment object, in reality, assessors are making assessments based on the results of interviews with knowledgeable individuals.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

Background Information for Assessment—*The organization identifies and arranges access to: (i) elements of the organization responsible for developing, documenting, disseminating, reviewing, and updating access control policies and associated procedures for implementing the policies; (ii) the access control policies for the information system and any associated access control-related procedures; (iii) individuals or groups responsible for the development, implementation, operation, and maintenance of access control procedures; (iv) any materials (e.g., security plans, records, schedules, assessment reports, after action reports, agreements, accreditation packages) associated with the implementation of access control procedures and operations; and (v) guidance on the number/percentage of objects to be assessed by type.*

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*AC-1.1. **Interview** selected organizational personnel with access control responsibilities to determine if access control policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required.*

Applicability: All impact levels

*AC-1.2. **Examine** the access control policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, and compliance for contingency operations.*

Applicability: All impact levels

*AC-1.3. **Examine** the access control procedures to determine if the procedures are sufficient to address all areas identified in the access control policy and all associated access controls.*

Applicability: All impact levels

*AC-1.4. **Examine** the access control policy and procedures to determine if the policy and procedures are updated periodically, when organizational reviews indicate updates are required.*

Applicability: Moderate and High impact levels

*AC-1.5. **Examine** the access control policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance.*

Applicability: Moderate and High impact levels

*AC-1.6. **Examine** access control policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the policy and procedures are disseminated, periodically reviewed, and updated.*

Applicability: Moderate and High impact levels

AC-1.7. ***Interview*** *selected organizational personnel with access control responsibilities and* ***examine*** *organizational records or documents to determine if anomalies or problems discovered by the organization in the content or application of the access control policy and procedures are being documented and the resulting information used to actively improve the policy and procedures.*

Applicability: High impact level

AC-1.8. ***Interview*** *selected organizational personnel with access control responsibilities and* ***examine*** *organizational records or documents to determine: (i) if the access control policy and procedure dissemination, reviews, and updates are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the dissemination, reviews, and updates of the policy and procedures are being documented and the resulting information used to actively improve the dissemination, review, and update processes on a continuous basis.*

Applicability: High impact level

AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency*].

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

*AC-2.1. **Examine** organizational records to determine if establishing, activating, modifying, reviewing, disabling, and removing accounts is being performed in accordance with the organization-defined frequency.*

Applicability: All impact levels

*AC-2.2. **Examine** an appropriately sized selection of active user accounts to determine if organizational procedures were followed to establish and activate the user accounts, including verifying that any organization-required documentation was completed.*

Applicability: All impact levels

*AC-2.3. **Examine** records of account reviews and modification instructions to determine if the prescribed actions have occurred in accordance with established procedures and were implemented on the information system.*

Applicability: All impact levels

*AC-2.4. **Examine** a sample set of system-generated records with user IDs and last login date for each account to determine if the last log-in date is beyond the [organizational-defined frequency], that the account is disabled.*

Applicability: All impact levels

*AC-2.5. **Examine** a list of recently separated or terminated employees to determine if accounts for these individuals have been removed according to established procedures, including verifying that any organization-required documentation was completed.*

Applicability: All impact levels

*AC-2.6. **Interview** selected organizational personnel with access control responsibilities to determine if the processes being applied are consistent with the documented account management procedures.*

Applicability: Moderate and High impact levels

*AC-2.7. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that information system accounts are managed correctly.*

Applicability: Moderate and High impact levels

*AC-2.8. **Interview** selected organizational personnel with account management responsibilities and **examine** organizational records or documents to determine: (i) if information system accounts are being managed consistently across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during account management are being documented and the resulting information used to actively improve the account management policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization employs automated mechanisms to support the management of information system accounts.

AC-2.9. ***Interview*** *selected organizational personnel with account management responsibilities and* ***examine*** *account management procedures to determine what information system account management functions are automated.*

Applicability: Moderate and High impact levels

AC-2.10. ***Examine*** *organizational records to determine if the automated account management functions identified in AC-2.9 are being employed in accordance with account management procedures and associated mechanism operating instructions.*

Applicability: Moderate and High impact levels

AC-2.11. ***Test*** *automated mechanisms(s) to determine if the automated account management functions identified in procedure AC-2.10 are functioning as intended.*

Applicability: Moderate and High impact levels

Control Enhancement:

(2) The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].

AC-2.12. ***Interview*** *selected organizational personnel with account management responsibilities and* ***examine*** *account management procedures to determine if temporary and emergency accounts are automatically terminated after [an organization-defined time period] for each type of account.*

Applicability: Moderate and High impact levels

AC-2.13. ***Examine*** *the information system configuration settings to determine if the settings are set to automatically terminate temporary and emergency accounts after [an organization-defined time period]*

Applicability: Moderate and High impact levels

AC-2.14. ***Examine*** *the temporary and emergency accounts on the information system to determine if any account is not terminated after [the organization-defined time period].*

Applicability: Moderate and High impact levels

AC-2.15. ***Test*** *the information system to determine if temporary and emergency accounts are automatically terminated after exceeding a set time period.*

Applicability: Moderate and High impact levels

Control Enhancement:

(3) The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].

AC-2.16. ***Interview*** *selected organizational personnel with account management responsibilities and* ***examine*** *account management procedures to determine if inactive accounts are automatically disabled after an [organization-defined time period].*

Applicability: Moderate and High impact levels

AC-2.17. ***Examine*** *the information system configuration settings to determine if the settings are set to automatically disable inactive accounts after [an organization-defined time period].*

Applicability: Moderate and High impact levels

AC-2.18. ***Examine*** *the inactive accounts on the information system to determine if any inactive accounts have not been disabled (i.e., if the last login date exceeds the [an organization-defined time period] for disabling inactive accounts).*

Applicability: Moderate and High impact levels

AC-2.19. ***Test*** *the information system to determine if inactive accounts are automatically disabled after exceeding a set inactive time period.*

Applicability: Moderate and High impact levels

Control Enhancement:

(4) The organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.

AC-2.20. ***Interview*** *selected organizational personnel with account management responsibilities and* ***examine*** *account management procedures to determine what automated mechanisms are employed to ensure that account creation, modification, disabling, and termination actions are audited and if the appropriate individuals are notified of these occurrences.*

Applicability: High impact level

AC-2.21. ***Examine*** *organizational records to determine if the automated mechanisms identified in procedure AC-2.20 are being employed in accordance with account management procedures and associated mechanism operating instructions.*

Applicability: High impact level

AC-2.22. ***Test*** *automated mechanism(s) to determine if each of the account actions identified in procedures AC-2.20 produce accurate and informative audit records, and each action, as required by the account management procedures, results in notification of appropriate individuals.*

Applicability: High impact level

AC-3 ACCESS ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

*AC-3.1. **Interview** selected organizational personnel with access control responsibilities to determine if the information system enforces assigned authorizations for controlling access to the system in accordance with applicable organizational policy.*

Applicability: All impact levels

*AC-3.2. **Examine** organizational records or documents to determine if user's access to the information system are authorized.*

Applicability: All impact levels

*AC-3.3. **Examine** access control mechanism to determine if the information system is configured to implement the organizational access control policy.*

Applicability: All impact levels

*AC-3.4. **Examine** the user access rights on the information system to determine if user privileges on the system are consistent with the documented user authorizations.*

Applicability: All impact levels

*AC-3.5. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that access controls are implemented correctly within the information system.*

Applicability: Moderate and High impact levels

*AC-3.6. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine: (i) if access enforcement is being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during access enforcement are being documented and the resulting information used to actively improve the access enforcement policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The information system ensures that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).

*AC-3.7. **Interview** selected organizational personnel with access control responsibilities to determine if only specified authorized personnel have access to the security functions and information of the information system.*

Applicability: Moderate and High impact levels

*AC-3.8. **Examine** system configuration documentation to determine if security functions have been explicitly defined for the information system.*

Applicability: Moderate and High impact levels

AC-3.9. ***Examine*** *organizational records and documents to determine if the personnel granted access to security functions and information have been properly authorized in accordance with organizational policy.*

Applicability: Moderate and High impact levels

AC-3.10. ***Test*** *selected accounts that have access to information system security functions to determine if the user privileges for those accounts function as documented in accordance with authorization requirements. .*

Applicability: Moderate and High impact levels

AC-4 INFORMATION FLOW ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

AC-4.1. ***Interview*** *selected organizational personnel with access control responsibilities to determine if permissible and impermissible information flow and authorization requirements for information are being applied in accordance with applicable organizational policy and procedures.*

Applicability: Moderate and High impact levels

AC-4.2. ***Examine*** *information system interconnection agreements to determine if the agreements address: (i) the types of permissible and impermissible flow of information between systems; and (ii) the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures.*

Applicability: Moderate and High impact levels

AC-4.3. ***Examine*** *information system configuration settings to determine if controls are in place to restrict the flow of information within the system and between interconnected systems in accordance with the applicable policy, procedures, and assigned authorizations.*

Applicability: Moderate and High impact levels

AC-4.4. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that information flow controls are implemented correctly within the information system and between interconnected systems.*

Applicability: Moderate and High impact levels

AC-4.5. ***Interview*** *selected organizational personnel with access control responsibilities and* ***examine*** *organizational records or documents to determine: (i) if information flow enforcement is being consistently applied across the information system and between interconnected systems on an ongoing basis; and (ii) if anomalies or problems encountered during information flow enforcement are being documented and the resulting information used to actively improve the information flow enforcement policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

AC-5 SEPARATION OF DUTIES

Control: The information system enforces separation of duties through assigned access authorizations.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

*AC-5.1. **Interview** selected organizational personnel with access control responsibilities to determine how the information system enforces separation of duties.*

Applicability: Moderate and High impact levels

*AC-5.2. **Examine** organizational charts and position descriptions to determine if personnel duties requiring the use of the information system, involve functions of significant criticality or sensitivity that should be subject to control by more than one individual.*

Applicability: Moderate and High impact levels

*AC-5.3. **Examine** selected information system accounts to determine if any user has access authorizations or privileges that may allow the user to perform multiple security functions (e.g., (i) mission functions and distinct information system support functions should be divided among different individuals/roles; (ii) different individuals perform information system support functions such as system management, systems programming, quality assurance/testing, configuration management, and network security; and (iii) security personnel who administer access control functions should not administer audit functions.)*

Applicability: Moderate and High impact levels

*AC-5.4. **Test** access control mechanisms by attempting to assign an individual user multiple roles within the information system to determine if the system allows a single user to perform multiple functions/roles.*

Applicability: Moderate and High impact levels

*AC-5.5. **Interview** selected organizational personnel with access control responsibilities to determine if separation of duties concepts are being applied in accordance with organizational policy and procedures.*

Applicability: Moderate and High impact levels

*AC-5.6. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the principle of separation of duties is correctly applied within the information system.*

Applicability: Moderate and High impact levels

*AC-5.7. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine: (i) if separation of duties is being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the implementation of separation of duties are being documented and the resulting information used to actively improve separation of duties policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

AC-6 LEAST PRIVILEGE

Control: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*AC-6.1. **Interview** selected organizational personnel with access control responsibilities to determine if the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.*

Applicability: Moderate and High impact levels

*AC-6.2 **Examine** organizational procedures or documents to determine what access rights/privileges are assigned to user tasks.*

Applicability: Moderate and High impact levels

*AC-6.3. **Examine** selected user accounts on the information system to determine if the access rights/privileges correspond to the authorized permissions on access documentation for specified tasks.*

Applicability: Moderate and High impact levels

*AC-6.4. **Interview** selected organizational personnel with access control responsibilities to determine if least privilege concepts are being applied in accordance with organizational policy and procedures.*

Applicability: Moderate and High impact levels

*AC-6.5. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the principle of least privileges is correctly applied within the information system.*

Applicability: Moderate and High impact levels

*AC-6.6. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine: (i) if the principle of least privilege is being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the implementation of least privilege are being documented and the resulting information used to actively improve least privilege policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control: The information system enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*] time period. The information system automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*], *delays next login prompt according to* [*Assignment: organization-defined delay algorithm.*]] when the maximum number of unsuccessful attempts is exceeded.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

AC-7.1. ***Examine*** *organizational records or documents to determine if the information system in accordance with access control policy and procedures: (i) enforces the maximum number of consecutive invalid access attempts within a certain period of time; (ii) automatically enforces a limit of an organization-defined number of consecutive invalid access attempts by a user during an organization-defined time period; and (iii) enforces automatic locks on the account/node for an organization-defined time period or delays the next login prompt according to an organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.*

Applicability: All impact levels

AC-7.2. ***Examine*** *the information system configuration settings to determine if the information system enforces organizational policy and procedures for unsuccessful login attempts.*

Applicability: All impact levels

AC-7.3. ***Test*** *the account lockout policy on selected user accounts by exceeding the maximum number of invalid login attempts within the organization-defined time period on the information system to determine if the information system locks the account/node.*

Applicability: Moderate and High impact levels

AC-7.4. ***Test*** *the account lockout policy on selected accounts by establishing initial lockout by exceeding the maximum number of invalid logon attempts, and then attempt to: (i) login to the account in less than the organization-defined delay lockout time period; and (ii) login to the account after the organization-defined lockout period to determine if the information system lockout/delay policy is being enforced.*

Applicability: Moderate and High impact levels

AC-7.4. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the information system enforces limits on unsuccessful login attempts and takes the correct actions when organization-defined limits are exceeded.*

Applicability: Moderate and High impact levels

AC-7.5. ***Interview*** *selected organizational personnel with access control responsibilities and* ***examine*** *organizational records or documents to determine: (i) if limitations on consecutive invalid access attempts are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the enforcement of unsuccessful login attempts and account locking are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with unsuccessful login attempts and account locking on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

AC-7.6. ***Examine*** *the information system configuration settings to determine if the information system is configured to automatically lock the account/nodes until released by the administrator when the maximum number of unsuccessful attempts is exceeded.*

Applicability: Optional

AC-7.7. ***Test*** *the account lockout mechanism by locking out selected accounts when exceeding the maximum number of invalid logon attempts, and then attempting to login to the accounts both before the administrator releases the locked accounts and after the administrator releases the locked accounts to determine if the information system administrator account lock release operates as intended.*

Applicability: Optional

AC-8 SYSTEM USE NOTIFICATION

Control: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

*AC-8.1. **Examine** the information system use notification message to determine if the message includes the following topics: (i) the user is accessing a U.S. Government information system; (ii) information system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the information system is prohibited and subject to criminal and civil penalties; (iv) use of the information system indicates consent to monitoring and recording; and (v) appropriate privacy and security notices (based on associated privacy and security policies or summaries).*

Applicability: All impact levels

*AC-8.2. **Interview** organizational personnel with access control responsibilities or examine organizational records or documents for approval of the information system use notification message before its use.*

Applicability: All impact levels

*AC-8.3. **Test** the system use notification message by accessing the login screen for the information system to determine if it remains on the screen until the user takes explicit actions to log on to the information system.*

Applicability: All impact levels

*AC-8.4. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the information system use notification message is implemented correctly.*

Applicability: Moderate and High impact levels

*AC-8.5. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine: (i) if system use notification is being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during system use notification are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with system use notification on a continuous basis.*

Applicability: High impact level

AC-9 PREVIOUS LOGON NOTIFICATION

Control: The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

Assessment Methods: Examine, Test

Assessment Objects: Specifications, Mechanisms

Assessment Procedure:

*AC-9.1. **Examine** the configuration settings of the information system to determine if upon successful logon, the system displays the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.*

Applicability: Optional

*AC-9.2. **Test** the information system by viewing a user logon process to the system to determine if upon successful logon, the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon are displayed.*

Applicability: Optional

*AC-9.3. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that previous logon notification is implemented correctly.*

Applicability: Optional

*AC-9.4. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine: (i) if previous logon notification is being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during previous logon notification are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with previous logon notification on a continuous basis.*

Applicability: Optional

AC-10 CONCURRENT SESSION CONTROL

Control: The information system limits the number of concurrent sessions for any user to [*Assignment: organization-defined number of sessions*].

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

AC-10.1. ***Examine*** *the configuration settings of the information system to determine if the system limits the number of concurrent sessions for users to an organization-defined number of sessions.*

Applicability: High impact level

AC-10.2. ***Test*** *the concurrent session control by attempting to exceed the organization-defined number of concurrent sessions with a valid user account.*

Applicability: High impact level

AC-10.3. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that concurrent session control is implemented correctly.*

Applicability: High impact level

AC-10.4. ***Interview*** *selected organizational personnel with access control responsibilities and* ***examine*** *organizational records or documents to determine: (i) if concurrent session control is being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the implementation of concurrent session control are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with concurrent session control on a continuous basis.*

Applicability: High impact level

AC-11 SESSION LOCK

Control: The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

*AC-11.1. **Examine** the configuration settings of the information system to determine if the system initiates a session lock until the user reestablishes access using appropriate identification and authentication procedures.*

Applicability: Moderate and High impact levels

*AC-11.2. **Test** the session lock mechanism by allowing a user session to remain inactive for the organization-defined period to determine if the session lock automatically occurs on the information system and that it remains in effect until the user reestablishes access using appropriate identification and authentication procedures.*

Applicability: Moderate and High impact levels

*AC-11.3. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that session locks are implemented correctly within the information system.*

Applicability: Moderate and High impact levels

*AC-11.4. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine: (i) if session lock is being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during session lock are being documented and the resulting information used to actively improve session lock policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a session after [*Assignment: organization-defined time period*] of inactivity.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

AC-12.1. ***Examine*** *the configuration settings of the information system to determine if the system automatically terminates a session after [an organization-defined time period] of inactivity.*

Applicability: Moderate and High impact levels

AC-12.2. ***Test*** *the session termination mechanism by allowing a valid user session to remain inactive for [an organization-defined time period] to determine if the session automatically terminates.*

Applicability: Moderate and High impact levels

AC-12.3. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that session terminations are implemented correctly within the information system.*

Applicability: Moderate and High impact levels

AC-12.4. ***Interview*** *selected organizational personnel with access control responsibilities and* ***examine*** *organizational records or documents to determine: (i) if session termination is being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during session termination are being documented and the resulting information used to actively improve the session termination policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

AC-13.1. ***Interview*** *selected organizational personnel responsible for supervision and reviewing activities of users to determine if the users usage of information system access controls are being reviewed and supervised.*

Applicability: All impact levels

AC-13.2. ***Examine*** *organizational records or documents to determine if unusual activity in usage of information system access controls are investigated, reported to appropriate officials, and resolved.*

Applicability: All impact levels

AC-13.3. ***Examine*** *organizational records of supervisory notices or disciplinary actions to users to determine if the organization is supervising user activities regarding the use and application of information system access controls.*

Applicability: Moderate and High impact levels

AC-13.4. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that supervision and review of user activities with respect to enforcement and usage of information system access controls are being implemented correctly.*

Applicability: Moderate and High impact levels

AC-13.5. ***Interview*** *selected organizational personnel with access control responsibilities and* ***examine*** *organizational records or documents to determine: (i) if user access control usage is being consistently supervised and reviewed across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the supervision and review of access control usage are being documented and the resulting information used to actively improve supervision and review policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization employs automated mechanisms to facilitate the review of user activities.

AC-13.6. ***Interview*** *selected organizational personnel with access control responsibilities to determine what automated mechanisms and automated functions are being employed to support and facilitate the review of user activities.*

Applicability: High impact level

AC-13.7. ***Examine*** *organizational records or documents to determine if automated mechanisms are being employed to support the review of user activities.*

Applicability: High impact level

AC-13.8. ***Test*** *the automated mechanism(s) within the information system to determine if each of the automated functions identified in AC-13.6 produces accurate and informative information to support and facilitate the review of user activities with respect to access control enforcement and usage.*

Applicability: High impact level

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization identifies specific user actions that can be performed on the information system without identification or authentication.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

*AC-14.1. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine what specific user actions can be performed on the information system without requiring identification and authentication.*

Applicability: All impact levels

*AC-14.2. **Examine** the configuration settings of the information system to determine if the system allows users to perform certain actions on the system without identifying and authenticating to the system in accordance with access control policy and procedures.*

Applicability: All impact levels

*AC-14.3. **Test** the information system by attempting to perform actions that are not authorized for a user that has not been identified or authenticated to the system, such as administrator functions.*

Applicability: Moderate and High impact levels

*AC-14.4. **Test** the information system by attempting to perform actions that are permitted without identification and authorization to determine if those actions can be performed in accordance with access control policy and procedures.*

Applicability: Moderate and High impact levels

*AC-14.5. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the organization defines and the information system correctly enforces permitted actions on the system without requiring user identification or authentication.*

Applicability: Moderate and High impact levels

*AC-14.6. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine: (i) if the actions permitted on the information system without requiring user identification or authentication are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the implementation of permitted actions without identification or authorization are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with permitted actions without identification or authorization on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

*AC-14.7. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine if the organization limits specific user actions that can be performed without identification and authentication to only mission-essential activities.*

Applicability: Moderate and High impact levels

AC-14.8. ***Examine*** *the configuration settings of the information system to determine if the system allows users to perform certain mission related actions without identifying and authenticating to the system.*

Applicability: Moderate and High impact levels

AC-14.9. ***Test*** *the information system by attempting to perform selected actions defined by access control policy and procedures as being the minimum actions necessary to accomplish mission objectives without identifying and authentication.*

Applicability: Moderate and High impact levels

AC-15 AUTOMATED MARKING

Control: The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

AC-15.1. ***Interview*** *selected organizational personnel with access control responsibilities to determine if standard naming conventions are used to identify any special dissemination, handling, or distribution instructions for information system output.*

Applicability: High impact level

AC-15.2. ***Examine*** *information system output to determine if the standard naming conventions are used to identify any special dissemination, handling, or distribution instructions.*

Applicability: High impact level

AC-15.3. ***Examine*** *the configuration of the information system to determine how the system automatically marks the output for any special disseminating, handling or distribution instructions.*

Applicability: High impact level

AC-15.4. ***Test*** *the automated marking control in the information system for selected outputs by executing processes to produce outputs to determine if the outputs are automatically marked using standard naming conventions and include any defined special dissemination, handling, or distribution instructions in accordance with automated marking policy and procedures.*

Applicability: High impact level

AC-15.5. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the output from the information system is correctly marked in order to achieve compliance with naming conventions and any special dissemination, handling, or distribution instructions.*

Applicability: High impact level

AC-15.6. ***Interview*** *selected organizational personnel with access control responsibilities and* ***examine*** *organizational records or documents to determine: (i) if automated marking of information system output is being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during automated marking are being documented and the resulting information used to actively improve the automated marking policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

AC-16 AUTOMATED LABELING

Control: The information system appropriately labels information in storage, in process, and in transmission.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

AC-16.1. ***Interview*** *selected organizational personnel with access control responsibilities to determine if the information system automatically labels information in storage, in process, and in transmission.*

Applicability: Optional

AC-16.2. ***Examine*** *information within the information system to determine if labels are accurately in place and in accordance with organizational policy and procedures.*

Applicability: Optional

AC-16.3. ***Examine*** *the configuration of the information system to determine if the system labels information in storage, in process, and in transmission.*

Applicability: Optional

AC-16.4. ***Test*** *the automated labeling mechanisms in the information system by displaying selected information in storage, after processing, and after transmission to determine if information is appropriately labeled in accordance with organizational policy and procedures.*

Applicability: Optional

AC-16.5. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the automated labeling is implemented correctly.*

Applicability: Optional

AC-16.6. ***Interview*** *selected organizational personnel with access control responsibilities and* ***examine*** *organizational records or documents to determine: (i) if automated labeling is being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during automated labeling are being documented and the resulting information used to actively improve the automated labeling policy, procedures, and processes on a continuous basis.*

Applicability: Optional

AC-17 REMOTE ACCESS

Control: The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms, Activities

Assessment Procedure:

*AC-17.1. **Interview** selected organizational personnel with access control responsibilities to determine if remote access is controlled, monitored, and authorized in accordance with organizational policy and procedures.*

Applicability: All impact levels

*AC-17.2. **Examine** organizational records or documents to determine: (i) if remote access is monitored on a periodic basis in accordance with organization policy; (ii) if remote access is restricted through dial-up connections or protects against unauthorized connections or subversion of unauthorized connections; (iii) if remote access is authorized and restricted to users with an operational need for access; and (iv) if remote access is restricted to only allow privileged access based on compelling operational needs.*

Applicability: All impact levels

*AC-17.3. **Examine** organizational records or documents to determine if remote access activity is being recorded in logs and reviewed periodically in accordance with the organizational policy and procedures.*

Applicability: All impact levels

*AC-17.4. **Examine** organizational records or documents to determine if remote access is documented and authorized by the appropriate organization officials.*

Applicability: All impact levels

*AC-17.5. **Examine** the configuration of the information system to determine if remote access to the system is employed to restrict access to the system.*

Applicability: All impact levels

*AC-17.6. **Examine** a system-generated list of user accounts with remote access and determine if the established procedures are followed to authorize remote access for the accounts.*

Applicability: All impact levels

*AC-17.7. **Test** the remote access controls by attempting to gain remote access to the information system using a valid system account that does not have remote access permissions.*

Applicability: Moderate and High impact levels

*AC-17.8. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that remote access controls are implemented correctly.*

Applicability: Moderate and High impact levels

AC-17.9. ***Interview*** *selected organizational personnel with access control responsibilities and* ***examine*** *organizational records or documents to determine: (i) if the remote access controls are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during remote access are being documented and the resulting information used to actively improve the remote access policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

AC-17.10. ***Interview*** *selected organizational personnel with access control responsibilities to determine what automated mechanisms and functions are employed to support and facilitate the monitoring and control of remote access methods.*

Applicability: Moderate and High impact levels

AC-17.11. ***Examine*** *organizational records or documents to determine if the automated mechanisms supporting the monitoring and control of remote access are being effectively employed in accordance with organizational policy and procedures.*

Applicability: Moderate and High impact levels

AC-17.12. ***Test*** *automated mechanism(s) to determine if each of the functions identified in AC-17.10 produce accurate and informative information, in accordance with remote access monitoring policy and procedures.*

Applicability: High impact level

Control Enhancement:

(2) The organization uses encryption to protect the confidentiality of remote access sessions.

AC-17.13. ***Interview*** *selected organizational personnel with access control responsibilities to determine if encryption is being used to protect the confidentiality of remote access sessions.*

Applicability: Moderate and High impact levels

AC-17.14. ***Examine*** *the configuration of the information system to determine if encryption is being used to protect the confidentiality of the remote access sessions.*

Applicability: Moderate and High impact levels

AC-17.15. ***Examine*** *a remote access connection to the information system to determine if the connection requires using organizational policy and procedures for encryption.*

Applicability: Moderate and High impact levels

Control Enhancement:

(3) The organization controls all remote accesses through a managed access control point.

AC-17.16. ***Interview*** *selected organizational personnel with access control responsibilities to determine if remote access is controlled through a centrally managed access control point.*

Applicability: Moderate and High impact levels

AC-17.17. ***Examine*** *the configuration of the information system to determine how remote access is controlled and if the organization controls access through a managed access control point.*

Applicability: Moderate and High impact levels

*AC-17.18. **Test** remote access controls by attempting to connect remotely to the information system without connecting through the managed access control point to determine if remote access can be achieved without following the organizational policy and procedures.*

Applicability: Moderate and High impact levels

AC-18 WIRELESS ACCESS RESTRICTIONS

Control: The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

*AC-18.1. **Interview** selected organizational personnel with access control responsibilities to determine if the organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; (ii) documents, monitors, and controls wireless access to the information system; and (iii) authorizes the use of wireless technologies.*

Applicability: Moderate and High impact levels

*AC-18.2. **Examine** access control policy and procedures to determine if the content of the policy and procedures are consistent with NIST Special Publication 800-48 and addresses usage, implementation, monitoring, and authorization of wireless technologies.*

Applicability: Moderate and High impact levels

*AC-18.3. **Examine** organizational records or documents to determine if wireless access usage is being tracked and monitored in accordance with organizational policy and procedures.*

Applicability: Moderate and High impact levels

*AC-18.4. **Examine** organizational records or documents to determine if wireless users have been authorized to access the information system.*

Applicability: Moderate and High impact levels

*AC-18.5. **Test** wireless access controls by attempting to access the information system through an unauthorized wireless connection to determine if the system is adequately protected from unauthorized wireless access.*

Applicability: Moderate and High impact levels

*AC-18.6. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the wireless access restrictions are implemented correctly.*

Applicability: Moderate and High impact levels

*AC-18.7. **Interview** selected organizational personnel with access control responsibilities and **examine** organizational records or documents to determine: (i) if wireless access restrictions are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the implementation of wireless access restrictions are being documented and the resulting information used to actively improve the wireless access policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization uses authentication and encryption to protect wireless access to the information system.

AC-18.8. ***Interview*** *selected organization personnel with access control responsibilities to determine if the organization uses authentication and encryption to protect wireless access to the information system.*

Applicability: Moderate and High impact level

AC-18.9. ***Examine*** *the configuration of the information system to determine if wireless access to the system is only permitted through authentication with encryption.*

Applicability: Moderate and High impact level

AC-18.10. ***Test*** *the wireless access restrictions by attempting to access the information system: (i) using an encrypted connection without authenticating to the system; and (ii) with a valid authentication mechanism over an unencrypted connection to determine if the access restrictions operate as intended.*

Applicability: Moderate and High impact level

AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES

Control: The organization: (i) establishes usage restrictions and implementation guidance for portable and mobile devices; and (ii) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications

Assessment Procedure:

AC-19.1. ***Interview*** *selected organizational personnel with access control responsibilities to determine if access controls for portable and mobile devices are being implemented in accordance with organizational policy and procedures.*

Applicability: Moderate and High impact levels

AC-19.2. ***Examine*** *organizational records or documents to determine: (i) if the organization establishes and documents restrictions and implementation guidance for portable and mobile devices to access organizational information systems; (ii) if the organization monitors and controls the use of portable and mobile devices on organizational information systems; and (iii) if appropriate organizational officials authorize the use of portable and mobile devices on organizational information systems.*

Applicability: Moderate and High impact levels

AC-19.3. ***Interview*** *selected organizational personnel with access to the information system to determine if the personnel are applying the usage restrictions and implementation guidance on the use of portable and mobile devices in accordance with organization policy and procedures.*

Applicability: Moderate and High impact levels

AC-19.4. ***Examine*** *organizational records or documents detailing the use of portable and mobile devices on organizational information systems to determine if personnel are following organizational policy and procedures on the use and implementation of portable and mobile devices.*

Applicability: Moderate and High impact levels

AC-19.5. ***Test*** *use of portable and mobile devices to access organizational information systems by attempting to connect an unauthorized portable or mobile device to an organizational information system to determine if organizational personnel can identify the unauthorized device.*

Applicability: Moderate and High impact levels

AC-19.6. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that access controls for portable and mobile devices are implemented correctly.*

Applicability: Moderate and High impact levels

AC-19.7. ***Interview*** *selected organizational personnel with access control responsibilities and* ***examine*** *organizational records or documents to determine: (i) if access controls for portable and mobile devices are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the implementation of access controls for mobile and portable devices are being documented and the resulting information used to actively improve access control policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization employs removable hard drives or cryptography to protect information residing on portable and mobile devices.

AC-19.8. ***Examine*** *organizational records or documents regarding the use of portable and mobile devices to determine if removable hard drives or cryptography are employed to protect information on the devices.*

Applicability: High impact level

AC-19.9. ***Interview*** *selected organizational personnel who use authorized portable or mobile devices to determine if they employ removable hard drives or cryptography to protect the information on the devices.*

Applicability: High impact level

AC-19.10. ***Examine*** *authorized portable or mobile devices to determine if the devices employ removable hard drives or cryptography to protect the information on the devices.*

Applicability: High impact level

AC-20 PERSONALLY OWNED INFORMATION SYSTEMS

Control: The organization restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

AC-20.1. ***Interview*** *selected organizational personnel with access control responsibilities to determine if the organization restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.*

Applicability: All impact levels

AC-20.2. ***Examine*** *the organizational records or documents to determine if the use of a personally owned information system meets the following minimum requirements as defined by the access control policy and procedures regarding: (i) the types of applications that can be accessed from personally owned information systems; (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; (iii) how other users of the personally owned information system will be prevented from accessing federal information; (iv) the use of virtual private networking (VPN) and firewall technologies; (v) the use of and protection against the vulnerabilities of wireless technologies; (vi) the maintenance of adequate physical security controls; (vii) the use of virus and spyware protection software; and (viii) how often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, spyware definitions).*

Applicability: All impact levels

AC-20.3. ***Interview*** *selected organizational personnel with access to the information system to determine if the personnel are adhering to the restrictions on the use of personally owned information systems for processing, storing, or transmitting federal information in accordance with access control policy and procedures.*

Applicability: All impact levels

AC-20.4. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the organization correctly restricts the use of personally owned information systems.*

Applicability: Moderate and High impact levels

AC-20.5. ***Interview*** *selected organizational personnel with access control responsibilities and* ***examine*** *organizational records or documents to determine: (i) if personally owned information system restrictions are being consistently applied across the organization on an ongoing basis; and (ii) if anomalies or problems encountered during the application of personally owned information system restrictions are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with restrictions on personally owned information systems on a continuous basis.*

Applicability: High impact level

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

[**Editor Note:** The security assessment procedures for this family are under development and will be included in subsequent drafts of Special Publication 800-53A.]

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

[**Editor Note:** The security assessment procedures for this family are under development and will be included in subsequent drafts of Special Publication 800-53A.]

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** OPERATIONAL

Background Information for Assessment—*The organization identifies and arranges access to: (i) elements of the organization responsible for developing, documenting, disseminating, reviewing, and updating security assessment, certification, and accreditation policies and associated procedures for implementing the policies; (ii) the security assessment, certification, and accreditation policies for the information system and any associated security assessment, certification, and accreditation-related procedures; (iii) individuals or groups responsible for the development, implementation, operation, and maintenance of security assessment, certification, and accreditation procedures; (iv) any materials (e.g., security plans, records, schedules, assessment reports, after action reports, agreements, accreditation packages) associated with the implementation of security assessment, certification, and accreditation procedures and operations; and (v) guidance on the number/percentage of objects to be assessed by type.*

CA-1 CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*CA-1.1. **Interview** selected organizational personnel with security assessment, certification, and accreditation responsibilities to determine if the security assessment, certification, and accreditation policies and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are reviewed by responsible parties within the organization; and (v) are updated periodically, if reviews indicate updates are required.*

Applicability: All impact levels

*CA-1.2. **Examine** the security assessment, certification, and accreditation policies to determine if the policies adequately address purpose, scope, roles, responsibilities, and compliance for security assessment, certification, and accreditation activities.*

Applicability: All impact levels

*CA-1.3. **Examine** the security assessment, certification, and accreditation procedures to determine if the procedures are sufficient to address all areas identified in the security assessment, certification, and accreditation policies and all associated security assessment, certification, and accreditation controls.*

Applicability: All impact levels

*CA-1.4. **Examine** the security assessment, certification, and accreditation policies and procedures to determine if the policies and procedures are updated periodically, when organizational reviews indicate updates are required.*

Applicability: Moderate and High impact levels

*CA-1.5. **Examine** the security assessment, certification, and accreditation policies to determine if the policies are consistent with the organization's mission and functions and associated laws, directives, policies, regulations, standards, and guidance.*

Applicability: Moderate and High impact levels

CA-1.6. ***Examine*** *certification, accreditation, and security assessment policies and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the policies and procedures are disseminated, periodically reviewed, and updated.*

Applicability: Moderate and High impact levels

CA-1.7. ***Interview*** *selected organizational personnel with certification, accreditation, and security assessment responsibilities and* ***examine*** *organizational records or documents to determine if anomalies or problems discovered by the organization in the content or application of the certification, accreditation, and security assessment policies and procedures are being documented and the resulting information used to actively improve the policies and procedures.*

Applicability: High impact level

CA-1.8. ***Interview*** *selected organizational personnel with certification, accreditation, and security assessment responsibilities and* ***examine*** *organizational records or documents to determine: (i) if the certification, accreditation, and security assessment policy and procedure dissemination, reviews, and updates are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the dissemination, reviews, and updates of the policies and procedures are being documented and the resulting information used to actively improve the dissemination, review, and update processes on a continuous basis.*

Applicability: High impact level

CA-2 SECURITY ASSESSMENTS

Control: The organization conducts an assessment of the security controls in the information system [A*ssignment: organization-defined frequency, at least annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*CA-2.1. **Interview** selected organizational personnel with security control assessment responsibilities to determine if an assessment of the security controls in the information system is conducted within the organization-defined frequency (at least annually).*

Applicability: Moderate and High impact levels

*CA-2.2. **Examine** selected security assessment reports to determine if the security controls in the information system are assessed for correct implementation, for intended operation, and for producing the desired outcome with respect to meeting the security requirements for the system in accordance with applicable policies and procedures.*

Applicability: Moderate and High impact levels

*CA-2.3. **Interview** selected organizational personnel with security assessment responsibilities to determine if their activities are consistent with the organization's security assessment procedures.*

Applicability: Moderate and High impact levels

*CA-2.4. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that security control assessments are conducted correctly within the information system.*

Applicability: Moderate and High impact levels

*CA-2.5. **Interview** selected organizational personnel with security assessment responsibilities and **examine** organizational records or documents to determine: (i) if security assessments are being consistently conducted on the information system on an ongoing basis; and (ii) if anomalies or problems encountered during security assessments are being documented and the resulting information used to actively improve security assessment policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

CA-3 INFORMATION SYSTEM CONNECTIONS

Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*CA-3.1. **Interview** selected organizational personnel with information system connection responsibilities and **examine** pertinent information system documentation to identify all information systems outside of the accreditation boundary (i.e., external information systems) that are connected to the information system.*

Applicability: All impact levels

*CA-3.2. **Examine** the information system connections procedures employed by the organization to determine if the procedures are consistent with NIST Special Publication 800-47.*

Applicability: All impact levels

*CA-3.3. **Interview** selected organizational personnel with responsibilities for monitoring/controlling connections to information systems outside of the accreditation boundary to determine if their activities are consistent with the organization's procedures for monitoring/controlling connections to those systems.*

Applicability: All impact levels

*CA-3.4. **Interview** selected organizational personnel with information system connection responsibilities and **examine** information system interconnection agreements and organizational records to determine if all connections to all information systems outside of the accreditation boundary are authorized and approved by appropriate organizational officials.*

Applicability: All impact levels

*CA-3.5. **Examine** selected organizational records used in monitoring/controlling connections to information systems outside of the accreditation boundary to determine if the activities are consistent with the organization's procedures for monitoring/controlling external information system connections.*

Applicability: Moderate and High impact levels

*CA-3.6. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that external connections to the information system are correctly authorized, monitored, and controlled.*

Applicability: Moderate and High impact levels

*CA-3.7. **Interview** selected organizational personnel with information system connection responsibilities and **examine** organizational records or documents to determine: (i) if information system connections are being consistently authorized, monitored, and controlled on an ongoing basis; and (ii) if anomalies or problems encountered during connection authorization, monitoring, and control are being documented and the resulting information used to actively improve the information system connection policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

CA-4 SECURITY CERTIFICATION

Control: The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*CA-4.1. **Interview** selected organizational personnel with security certification responsibilities to determine if a certification process is defined that determines the effectiveness of each security control in the information system regarding correct implementation, intended operation, and producing the desired outcome with respect to meeting the security requirements for the system.*

Applicability: All impact levels

*CA-4.2. **Examine** the security certification procedures to determine if the procedures are consistent with NIST Special Publications 800-37 and 800-53A.*

Applicability: All impact levels

*CA-4.3. **Examine** the security certification documentation to determine if contents include the results of security control assessments and specific actions taken or planned to correct deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system.*

Applicability: All impact levels

*CA-4.4. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the security certification of the information system is conducted correctly.*

Applicability: Moderate and High impact levels

*CA-4.5. **Interview** selected organizational personnel with security certification responsibilities and **examine** organizational records or documents to determine: (i) if security certifications are being consistently conducted on the information system on an ongoing basis; and (ii) if anomalies or problems encountered during security certifications are being documented and the resulting information used to actively improve the security certification policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

CA-5 PLAN OF ACTION AND MILESTONES

Control: The organization develops and updates [*Assignment: organization-defined frequency*], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*CA-5.1. **Interview** selected organizational personnel with plan of action and milestones responsibilities to determine if the organization develops and updates an action plan for the information system within the organization-defined frequency.*

Applicability: All impact levels

*CA-5.2. **Examine** selected security assessment reports for deficiencies noted during the assessment of the security controls in the information system; **examine** the corresponding plan of action to determine if the plan documents the organization's planned, implemented, and evaluated remedial actions to correct noted deficiencies and to reduce or eliminate known vulnerabilities in the system.*

Applicability: All impact levels

*CA-5.3. **Examine** selected action plan milestones to determine if the organization's planned, implemented, and evaluated remedial actions to correct deficiencies in the information system security controls show evidence that milestones are being met and that the plan is being implemented.*

Applicability: All impact levels

*CA-5.4. **Examine** selected security controls with deficiencies noted in the plan of action and milestones to determine if the deficiencies are corrected as defined by the action plan.*

Applicability: Moderate and High impact levels

*CA-5.5. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that a plan of action and milestones for the information system is correctly developed, implemented, and updated.*

Applicability: Moderate and High impact levels

*CA-5.6. **Interview** selected organizational personnel with security assessment responsibilities and **examine** organizational records or documents to determine: (i) if a plan of action and milestones is being consistently developed and updated for the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the development and updating of the plan of action and milestones are being documented and the resulting information used to actively improve the policy, procedures, and development processes associated with the plan of action and milestones on a continuous basis.*

Applicability: High impact level

CA-6 SECURITY ACCREDITATION

Control: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [*Assignment: organization-defined frequency*]. A senior organizational official signs and approves the security accreditation.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*CA-6.1. **Interview** selected organizational personnel with security accreditation responsibilities and **examine** accreditation documentation to determine if an accreditation process is defined that authorizes (i.e., accredits) the information system for processing before operations, and updates the authorization within the organization-defined frequency.*

Applicability: All impact levels

*CA-6.2. **Examine** the information system accreditation procedures to determine if the procedures are consistent with NIST Special Publication 800-37.*

Applicability: All impact levels

*CA-6.3. **Examine** organizational records to determine if a senior organizational official signs and approves the security accreditation.*

Applicability: All impact levels

*CA-6.4. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the security accreditation of the information system is conducted correctly.*

Applicability: Moderate and High impact levels

*CA-6.5. **Interview** selected organizational personnel with security accreditation responsibilities and **examine** appropriate organizational records or documents to determine: (i) if security accreditations are being consistently conducted on the information system on an ongoing basis; and (ii) if anomalies or problems encountered during security accreditations are being documented and the resulting information used to actively improve the security accreditation policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

CA-7 CONTINUOUS MONITORING

Control: The organization monitors the security controls in the information system on an ongoing basis.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*CA-7.1. **Interview** selected organizational personnel with security control monitoring responsibilities to determine if security controls are being monitored according to defined procedures on an ongoing basis.*

Applicability: All impact levels

*CA-7.2. **Examine** the security control monitoring procedures to determine if the procedures are consistent with NIST Special Publication 800-37.*

Applicability: All impact levels

*CA-7.3. **Examine** selected organizational records to determine: (i) if designated security controls are assessed; (ii) if changes to or deficiencies in the operation of the security controls are analyzed for impact, documented, and reported; and (iii) if adjustments are made to the information system security plan and plan of action and milestones, as appropriate.*

Applicability: Moderate and High impact levels

*CA-7.4. **Interview** selected organizational personnel with security control monitoring responsibilities to determine if their activities are consistent with the organization's security control monitoring procedures.*

Applicability: Moderate and High impact levels

*CA-7.5. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that security control monitoring within the information system is conducted correctly.*

Applicability: Moderate and High impact levels

*CA-7.6. **Interview** selected organizational personnel with security control monitoring responsibilities and **examine** organizational records or documents to determine: (i) if security control monitoring is being consistently conducted across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during security control monitoring are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with security control monitoring on a continuous basis.*

Applicability: High impact level

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

[**Editor Note:** The security assessment procedures for this family are under development and will be included in subsequent drafts of Special Publication 800-53A.]

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

Background Information for Assessment—*The organization identifies and arranges access to: (i) elements of the organization responsible for developing, documenting, disseminating, reviewing, and updating the contingency planning policy and associated procedures for implementing the policy; (ii) the contingency plan for the information system and any associated contingency-related procedures; (iii) individuals or groups responsible for the implementation and operation of the contingency plan and procedures; (iv) any materials (e.g., records, schedules, after action reports, agreements) associated with the implementation of the contingency plan or contingency operations; and (v) guidance on the number/percentage of objects to be assessed by type.*

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*CP-1.1. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine if contingency planning policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required.*

Applicability: All impact levels

*CP-1.2. **Examine** the contingency planning policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, and compliance for contingency operations.*

Applicability: All impact levels

*CP-1.3. **Examine** the contingency planning procedures to determine if the procedures are sufficient to address all areas identified in the contingency planning policy and all associated contingency planning controls.*

Applicability: All impact levels

*CP-1.4. **Examine** the contingency planning policy and procedures to determine if the policy and procedures are updated periodically, when organizational reviews indicate updates are required.*

Applicability: Moderate and High impact levels

*CP-1.5. **Examine** the contingency planning policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance.*

Applicability: Moderate and High impact levels

*CP-1.6. **Examine** the contingency planning policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the policy and procedures are disseminated, periodically reviewed, and updated.*

Applicability: Moderate and High impact levels

CP-1.7. ***Interview*** *selected organizational personnel with contingency planning and plan implementation responsibilities and* ***examine*** *organizational records or documents to determine if anomalies or problems discovered by the organization in the content or application of the contingency planning policy and procedures are being documented and the resulting information used to actively improve the policy and procedures.*

Applicability: High impact level

CP-1.8. ***Interview*** *selected organizational personnel with contingency planning and plan implementation responsibilities and* ***examine*** *organizational records or documents to determine: (i) if the contingency planning policy and procedure dissemination, reviews, and updates are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the dissemination, reviews, and updates of the policy and procedures are being documented and the resulting information used to actively improve the dissemination, review, and update processes on a continuous basis.*

Applicability: High impact level

CP-2 CONTINGENCY PLAN

Control: The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*CP-2.1. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine if the contingency plan: (i) exists; (ii) is disseminated to appropriate elements within the organization; and (iii) is reviewed and approved by responsible officials within the organization.*

Applicability: All impact levels

*CP-2.2. **Examine** the contingency plan to determine if the content of the plan is consistent with NIST Special Publication 800-34 and addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system.*

Applicability: All impact levels

*CP-2.3. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine if the contingency plan is consistent with the organization's contingency planning policy and procedures.*

Applicability: Moderate and High impact levels

*CP-2.4. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine if key operating elements within the organization are ready to implement the contingency plan.*

Applicability: Moderate and High impact levels

*CP-2.5. **Examine** the contingency plan to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the plan is implemented correctly.*

Applicability: Moderate and High impact levels

*CP-2.6. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine: (i) if the contingency plan is being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the development or implementation of the contingency plan are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with the contingency plan on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization coordinates contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).

*CP-2.7. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine if contingency plan development is coordinated with other organizational elements responsible for related plans identified by the organization.*

Applicability: Moderate and High impact levels

CP-2.8. ***Interview*** *selected organizational personnel with responsibilities for developing plans related to the contingency plan to determine if contingency plan development is coordinated with the related plans and the contingency plan supports the requirements in the related plans.*

Applicability: Moderate and High impact levels

CP-3 CONTINGENCY TRAINING

Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

CP-3.1. ***Examine*** *organizational records to determine: (i) if contingency training is provided to individuals implementing the contingency plan; (ii) if records include the type of contingency training received and the date completed; and (iii) if initial and refresher training of individual roles and responsibilities is provided in accordance with organization-defined frequency, at least annually.*

Applicability: Moderate and High impact levels

CP-3.2. ***Examine*** *training material for selected contingency roles and responsibilities to determine if the training material addresses the procedures/activities for implementing those roles and responsibilities.*

Applicability: Moderate and High impact levels

CP-3.3. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that contingency training for the information system is conducted correctly.*

Applicability: Moderate and High impact levels

CP-3.4. ***Interview*** *selected organizational personnel with contingency planning and plan implementation responsibilities and* ***examine*** *organizational records or documents to determine: (i) if the contingency training is being consistently conducted across the organization on an ongoing basis; and (ii) if anomalies or problems encountered during contingency training are being documented and the resulting information used to actively improve the contingency training policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement

(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

CP-3.5. ***Interview*** *selected organizational personnel with contingency planning and plan implementation responsibilities and* ***examine*** *contingency plan/procedures to determine what contingency training events are simulated and how these events improve the training process.*

Applicability: High impact level

CP-3.6. ***Examine*** *organizational records/documentation to determine if the simulated events identified by the organization are being employed in accordance with contingency training plans/procedures.*

Applicability: High impact level

CP-3.7. ***Test*** *selected simulated events to determine if organizational personnel respond as expected to the simulated crisis situation.*

Applicability: High impact level

Control Enhancement:

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

CP-3.8. ***Interview*** *selected organizational personnel with contingency planning and plan implementation responsibilities and* ***examine*** *contingency plans/procedures to determine what contingency training functions are automated and how the automated mechanisms improve the training process.*

Applicability: Optional

CP-3.9. ***Examine*** *organizational records/documentation to determine if the automated mechanisms identified by the organization are being employed in accordance with contingency training plans/procedures.*

Applicability: Optional

CP-3.10. ***Test*** *selected automated mechanisms to determine if the mechanisms are operating as intended.*

Applicability: Optional

CP-4 CONTINGENCY PLAN TESTING

Control: The organization tests the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*CP-4.1. **Examine** organizational records to determine if the organization tests its contingency plan in accordance with organization-defined frequency, at least annually, and the results of the tests are documented.*

Applicability: Moderate and High impact levels

*CP-4.2. **Examine** organizational records to determine if the contingency plan tests (or exercises) address key aspects of the plan and if the tests (or exercises) confirm that the plan objectives are met.*

Applicability: Moderate and High impact levels

*CP-4.3. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine the overall effectiveness of the contingency plan and the readiness of the organization to execute the plan.*

Applicability: Moderate and High impact levels

*CP-4.4. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records to determine if the contingency plan test results are being reviewed and if corrective actions are being taken.*

Applicability: Moderate and High impact levels

*CP-4.5. **Examine** organizational policy and procedures to determine if specific parties are responsibility and specific actions are defined to ensure that contingency plan testing for the information system is conducted correctly.*

Applicability: Moderate and High impact levels

*CP-4.6. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine: (i) if the contingency plan testing is being consistently conducted across the organization on an ongoing basis; and (ii) if anomalies or problems encountered during contingency plan testing are being documented and the resulting information used to actively improve the testing policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).

*CP-4.7. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine if contingency plan testing is coordinated with other organizational elements responsible for related plans identified by the organization.*

Applicability: Moderate and High impact levels

CP-4.8. ***Interview*** *selected organizational personnel with responsibilities for developing related plans to determine if contingency plan testing is coordinated with the testing associated with the related plans.*

Applicability: Moderate and High impact levels

Control Enhancement:

(2) The organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

CP-4.9. ***Interview*** *selected organizational personnel with contingency planning and plan implementation responsibilities to determine if the personnel are familiar with the alternate processing site and the capabilities available at the site.*

Applicability: High impact level

CP-4.10. ***Examine*** *organizational records to determine if contingency plan testing is being performed at the alternate site and if the site can successfully support contingency operations.*

Applicability: High impact level

Control Enhancement:

(3) The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.

CP-4.11. ***Interview*** *selected organizational personnel with contingency planning and plan implementation responsibilities to determine what automated mechanisms are employed to support contingency plan testing and how the mechanisms improve the testing process.*

Applicability: Optional

CP-4.12. ***Examine*** *organizational documentation to determine if the automated mechanisms supporting contingency plan testing are employed as defined in the contingency plan/procedures.*

Applicability: Optional

CP-5 CONTINGENCY PLAN UPDATE

Control: The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*CP-5.1. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine if the contingency plan is updated in accordance with organization-defined frequency (at least annually).*

Applicability: All impact levels

*CP-5.2. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** records of information system/organizational changes or problems encountered during contingency plan implementation, execution, or testing to determine if needed changes are reflected in the contingency plan.*

Applicability: All impact levels

*CP-5.3. **Examine** the contingency plan to determine if the revised plan reflects the needed changes based on the organization's experiences during plan implementation, execution, and testing.*

Applicability: All impact levels

*CP-5.4. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that contingency plan reviews and updates for the information system are conducted correctly.*

Applicability: Moderate and High impact levels

*CP-5.5. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine: (i) if the contingency plan is being consistently reviewed and updated on an ongoing basis; and (ii) if anomalies or problems encountered during the plan update process are being documented and the resulting information used to actively improve the plan update policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

CP-6 ALTERNATE STORAGE SITES

Control: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*CP-6.1. **Interview** alternate storage site administrators and **examine** alternate storage site agreements to determine if agreements are currently in place.*

Applicability: Moderate and High impact levels

*CP-6.2. **Examine** each alternate storage site to determine if the site is available and accessible in accordance with the alternate site agreement.*

Applicability: Moderate and High impact levels

*CP-6.3. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that necessary alternate storage site agreements are correctly initiated to permit information system backup operations.*

Applicability: Moderate and High impact levels

*CP-6.4. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine: (i) if alternate storage site agreements are being consistently reviewed on an ongoing basis; and (ii) if anomalies or problems encountered during the development or review of alternate storage site agreements are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with the development or review of alternate storage site agreements on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.

*CP-6.5. **Examine** the organization's contingency plan to determine if the plan identifies the primary storage site hazards.*

Applicability: Moderate and High impact levels

*CP-6.6. **Examine** the organization's alternate storage site to determine if the site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary storage site.*

Applicability: Moderate and High impact levels

Control Enhancement:

(2) The alternate storage site is configured to facilitate timely and effective recovery operations.

*CP-6.7. **Examine** the alternate storage site agreement to determine if the agreement specifies configuration requirements to facilitate timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives).*

Applicability: High impact level

CP-6.8. ***Test*** *the alternate storage site operations to determine if the alternate site is configured to enable timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives) in accordance with the provisions of alternate storage site agreement.*

Applicability: High impact level

Control Enhancement:

(3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-6.9. ***Examine*** *the organization's contingency plan to determine if the plan: (i) identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and (ii) defines explicit mitigation actions for those accessibility problems.*

Applicability: High impact level

CP-6.10. ***Test*** *the organization's mitigation actions for accessing the alternate storage site in the event of an area-wide disruption or disaster to determine if the mitigation actions resolve the associated accessibility problems.*

Applicability: High impact level

CP-7 ALTERNATE PROCESSING SITES

Control: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [*Assignment: organization-defined time period*] when the primary processing capabilities are unavailable.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*CP-7.1. **Examine** alternate processing site agreements and **interview** alternate processing site administrators to determine if agreements are currently in place to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.*

Applicability: Moderate and High impact levels

*CP-7.2. **Examine** each alternate processing site to determine if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period.*

Applicability: Moderate and High impact levels

*CP-7.3. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that necessary alternate processing site agreements are correctly initiated to permit the resumption of information system operations for critical mission/business functions within an organization-defined time period.*

Applicability: Moderate and High impact levels

*CP-7.4. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine: (i) if alternate processing site agreements are being consistently reviewed on an ongoing basis; and (ii) if anomalies or problems encountered during the development or review of alternate processing site agreements are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with the development or review of alternate processing site agreements on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards.

*CP-7.5. **Examine** the organization's contingency plan to determine if the plan identifies the primary processing site hazards.*

Applicability: Moderate and High impact levels

*CP-7.6. **Examine** the organization's alternate processing site to determine if the site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary processing site.*

Applicability: Moderate and High impact levels

Control Enhancement:

(2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

*CP-7.7. **Examine** the organization's contingency plan to determine if the plan: (i) identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and (ii) defines explicit mitigation actions for those accessibility problems.*

Applicability: High impact level

*CP-7.8. **Test** the organization's mitigation actions for accessing the alternate processing site in the event of an area-wide disruption or disaster to determine if the mitigation actions resolve the associated accessibility problems.*

Applicability: High impact level

Control Enhancement:

(3) Alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.

*CP-7.9. **Examine** alternate processing site agreements and **interview** alternate processing site administrators to determine if agreements are currently in place and contain priority of service provisions in accordance with the organization's availability requirements.*

Applicability: High impact level

Control Enhancement:

(4) The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.

*CP-7.10. **Examine** alternate processing site agreements to determine if the agreements specify the configuration requirements needed to support the minimum required operational capability of the organization.*

Applicability: High impact level

*CP-7.11. **Test** selected components of the information system at the alternate processing site to determine if the site is configured to support the minimum required operational capability of the organization and is ready to use as the operational site.*

Applicability: High impact level

CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*CP-8.1. **Examine** alternate telecommunication service agreements and **interview** alternate telecommunication service administrators to determine if agreements are currently in place to permit the resumption of telecommunication services for critical mission/business functions within organization-defined time period when the primary telecommunications capabilities are unavailable.*

Applicability: Moderate and High impact levels

*CP-8.2. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that necessary alternate telecommunications service agreements are correctly initiated to permit the resumption of information system operations for critical mission/business functions within an organization-defined time period.*

Applicability: Moderate and High impact levels

*CP-8.3. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine: (i) if primary and alternate telecommunications service agreements are being consistently reviewed on an ongoing basis; and (ii) if anomalies or problems encountered during the development or review of primary and alternate telecommunications service agreements are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with the development or review of primary and alternate telecommunications service agreements on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements.

*CP-8.4. **Examine** primary and alternate telecommunication service agreements and **interview** primary and alternate telecommunication service administrators to determine if agreements contain priority of service provisions in accordance with the availability requirements defined in the organization's contingency plan..*

Applicability: Moderate and High impact levels

Control Enhancement:

(2) Alternate telecommunications services do not share a single point of failure with primary telecommunications services.

*CP-8.5. **Examine** primary and alternate telecommunication service agreements and **interview** primary and alternate telecommunication service administrators to determine if the alternate telecommunication services share a single point of failure with the primary telecommunications services.*

Applicability: Moderate and High impact levels

Control Enhancement:

(3) Alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.

CP-8.6. ***Examine*** *the alternate telecommunication service provider's site to determine if the site is sufficiently separated from the primary telecommunication service provider's site so as not to be susceptible to the same hazards identified at the primary telecommunication service provider's site.*

Applicability: High impact level

Control Enhancement:

(4) Primary and alternate telecommunications service providers have adequate contingency plans.

CP-8.7. ***Examine*** *the contingency plans from the primary and alternate telecommunication service providers and* ***interview*** *the primary and alternate telecommunication service administrators to determine if the contingency plans are adequate.*

Applicability: High impact level

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*] and stores backup information at an appropriately secured location.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*CP-9.1. **Interview** organizational personnel responsible for information system backup to determine if the user-level and system-level information (including system state information) that is required to be backed up is defined and the location for storing backup information is identified.*

Applicability: All impact levels

*CP-9.2. **Examine** information system backup procedures to determine if procedures are defined for backing up required user-level and system-level information (including system state information) within organization-defined frequency, and storing backup information in a secure location.*

Applicability: All impact levels

*CP-9.3. **Examine** selected information backup media, or selected records of such back up if available, to determine if the required user-level and system-level information (including system state information) is backed up within the organization-defined frequency and stored in the designated location in accordance with information system backup procedures.*

Applicability: All impact levels

*CP-9.4. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that information system backups are conducted correctly.*

Applicability: Moderate and High impact levels

*CP-9.5. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine: (i) if information system backups are being consistently conducted across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during information system backup operations are being documented and the resulting information used to actively improve the system backup policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization tests backup information [*Assignment: organization-defined frequency*] to ensure media reliability and information integrity.

*CP-9.6. **Examine** test results from organization testing of backup information to determine if testing is conducted within the organization-defined frequency, and testing results indicate backup media reliability and information integrity.*

Applicability: Moderate and High impact levels

Control Enhancement:

(2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.

*CP-9.7. **Examine** organizational records to determine if testing is conducted with selected backup information in the restoration of information system functions as part of contingency plan testing.*

Applicability: High impact level

Control Enhancement:

(3) The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

*CP-9.8. **Examine** back up storage location to determine if back up copies of the operating system and other critical information system software are stored in a fire-rated container that is not collocated with the operational software.*

Applicability: High impact level

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*CP-10.1. **Interview** organizational personnel responsible for employing mechanisms to recover and reconstitute the information system to its original state to determine if mechanisms and procedures are available and are being applied.*

Applicability: All impact levels

*CP-10.2. **Examine** information system recovery and reconstitution procedures to determine if means are identified for capturing the system's operational state including all system parameters, patches, configuration settings and application and system software prior to information system disruption or failure.*

Applicability: All impact levels

*CP-10.3. **Examine** information system recovery and reconstitution procedures to determine if the procedures require the system be tested upon information system recovery and reconstitution.*

Applicability: All impact levels

*CP-10.4. **Test** information system recovery and reconstitution mechanisms using selected components of the information system to determine if the system can be fully restored to its original operational state.*

Applicability: All impact levels

*CP-10.5. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that information system recovery and reconstitution are conducted correctly.*

Applicability: Moderate and High impact levels

*CP-10.6. **Interview** selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine: (i) if recovery and reconstitution operations are being consistently conducted across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during information system recovery and reconstitution are being documented and the resulting information used to actively improve the recovery and reconstitution policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.

*CP-10.7. **Examine** test results or organizational records from contingency plan testing to determine if the organization includes a full recovery and reconstitution of the information system with the most recent backups as part of contingency plan testing.*

Applicability: High impact level

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

[**Editor Note:** The security assessment procedures for this family are under development and will be included in subsequent drafts of Special Publication 800-53A.]

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

Background Information for Assessment—*The organization identifies and arranges access to: (i) elements of the organization responsible for developing, documenting, disseminating, reviewing, and updating the incident response policy and associated procedures for implementing the policy; (ii) the incident response plan for the information system and any associated incident response-related procedures; (iii) individuals or groups responsible for the development, implementation, operation, and maintenance of the incident response plan and procedures; (iv) any materials (e.g., incident reports, follow-up meeting notes) associated with the implementation of the incident response plan or incident response operations; and (v) guidance on the number/percentage of objects to be assessed by type.*

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*IR-1.1. **Interview** selected organizational personnel with incident response responsibilities to determine if the incident response policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required.*

Applicability: All impact levels

*IR-1.2. **Examine** the incident response policy to determine if the policy addresses purpose, scope, roles, responsibilities, and compliance for incident response operations.*

Applicability: All impact levels

*IR-1.3. **Examine** the incident response procedures to determine if the procedures are sufficient to address all areas identified in the incident response policy and all associated incident response controls.*

Applicability: All impact levels

*IR-1.4. **Examine** the incident response policy and procedures to determine if the policy and procedures are updated periodically, when organizational reviews indicate updates are required.*

Applicability: Moderate and High impact levels

*IR-1.5. **Examine** the incident response policy to determine if the policy is consistent with the organization's mission and functions and associated laws, directives, policies, regulations, standards, and guidance.*

Applicability: Moderate and High impact levels

*IR-1.6. **Examine** incident response policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the policy and procedures are disseminated, periodically reviewed, and updated.*

Applicability: Moderate and High impact levels

IR-1.7. ***Interview*** *selected organizational personnel with incident response responsibilities and* ***examine*** *organizational records or documents to determine if anomalies or problems discovered by the organization in the content or application of the incident response policy and procedures are being documented and the resulting information used to actively improve the policy and procedures.*

Applicability: High impact level

IR-1.8. ***Interview*** *selected organizational personnel with incident response responsibilities and* ***examine*** *organizational records or documents to determine: (i) if the incident response policy and procedure dissemination, reviews, and updates are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the dissemination, reviews, and updates of the policy and procedures are being documented and the resulting information used to actively improve the dissemination, review, and update processes on a continuous basis.*

Applicability: High impact level

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

IR-2.1. ***Examine*** *organizational records to determine: (i) if incident response training is provided to individuals implementing the incident response plan/procedures; (ii) if records include the type of incident response training received and the date completed; and (iii) if initial and refresher training of individual roles and responsibilities is provided in accordance with organization-defined frequency, at least annually.*

Applicability: Moderate and High impact levels

IR-2.2. ***Examine*** *training material for selected incident response roles and responsibilities to determine if the material addresses the procedures/activities for implementing those roles and responsibilities.*

Applicability: Moderate and High impact levels

IR-2.3. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that incident response training for the information system is conducted correctly.*

Applicability: Moderate and High impact levels

IR-2.4. ***Interview*** *selected organizational personnel with incident response responsibilities and* ***examine*** *organizational records or documents to determine: (i) if the incident response training is being consistently conducted across the organization on an ongoing basis; and (ii) if anomalies or problems encountered during incident response training are being documented and the resulting information used to actively improve the training policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement

(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

IR-2.5. ***Interview*** *selected organizational personnel with incident response responsibilities and* ***examine*** *incident response plan/procedures to determine what incident response training events are simulated and how these events improve the training process.*

Applicability: High impact level

IR-2.6. ***Examine*** *organizational records/documentation to determine if the simulated events identified by the organization are being employed in accordance with incident response training plans/procedures.*

Applicability: High impact level

IR-2.7. ***Test*** *selected simulated events to determine if organizational personnel respond as expected to the simulated incident situation.*

Applicability: High impact level

Control Enhancement:

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

IR-2.8. ***Interview*** *selected organizational personnel with incident response responsibilities and* ***examine*** *incident response plans/procedures to determine what incident response training functions are automated and how the automated mechanisms improve the training process.*

Applicability: Optional

IR-2.9. ***Examine*** *organizational records/documentation to determine if the automated mechanisms identified by the organization are being employed in accordance with incident response training plans/procedures.*

Applicability: Optional

IR-2.10. ***Test*** *selected automated mechanisms to determine if the mechanisms are operating as intended.*

Applicability: Optional

IR-3 INCIDENT RESPONSE TESTING

Control: The organization tests the incident response capability for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and exercises*] to determine the incident response effectiveness and documents the results.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

IR-3.1. ***Examine*** *organizational records to determine if the organization tests its incident response capability in accordance with organization-defined frequency, at least annually, and the results of the tests are documented.*

Applicability: Moderate and High impact levels

IR-3.2. ***Examine*** *organizational incident response tests to determine if the tests (or exercises) address key aspects of the incident response capability.*

Applicability: Moderate and High impact levels

IR-3.3. ***Interview*** *selected organizational personnel with incident response responsibilities and* ***examine*** *organizational records or documents and incident response test results to determine if the organization's analysis of the test results indicates that the incident response capability is effective.*

Applicability: Moderate and High impact levels

IR-3.4. ***Interview*** *selected organizational personnel with incident response responsibilities and* ***examine*** *organizational records to determine if the incident response test results are being reviewed and if corrective actions are being taken.*

Applicability: Moderate and High impact levels

IR-3.5. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that incident response testing for the information system is conducted correctly.*

Applicability: Moderate and High impact levels

IR-3.6. ***Interview*** *selected organizational personnel with incident response responsibilities and* ***examine*** *organizational records or documents to determine: (i) if incident response testing is being consistently conducted across the organization on an ongoing basis; and (ii) if anomalies or problems encountered during incident response testing are being documented and the resulting information used to actively improve the testing policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.

IR-3.7. ***Interview*** *selected organizational personnel with incident response responsibilities to determine what automated mechanisms are employed to support incident response testing and how the mechanisms improve the testing process.*

Applicability: Optional

IR-3.8. ***Examine*** *organizational documentation to determine if the automated mechanisms supporting incident response testing are employed as defined in the incident response procedures.*

Applicability: Optional

IR-3.9. ***Test*** *selected incident response mechanisms to determine if the mechanisms are operating as intended.*

Applicability: Optional

IR-4 INCIDENT HANDLING

Control: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms, Activities

Assessment Procedure:

*IR-4.1. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records or documents to determine if incident handling activities for security incidents that include preparation, detection and analysis, containment, eradication, and recovery are implemented.*

Applicability: All impact levels

*IR-4.2. **Examine** records of activity for (or actual organizational personnel engaged in) incident handling to determine if the personnel are following designated procedures for conducting such activities.*

Applicability: Moderate and High impact levels

*IR-4.3. **Examine** records of activity for incident handling preparation (or actual organizational incident handling preparatory measures) to determine if incident handling requirements are met.*

Applicability: Moderate and High impact levels

*IR-4.4. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that incident handling for the information system is conducted correctly.*

Applicability: Moderate and High impact levels

*IR-4.5. **Interview** selected organizational personnel with incident handling responsibilities and **examine** appropriate organizational records or documents to determine: (i) if incident handling is being consistently conducted across the organization on an ongoing basis; and (ii) if anomalies or problems encountered during incident handling are being documented and the resulting information used to actively to improve incident handling policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization employs automated mechanisms to support the incident handling process.

*IR-4.6. **Interview** selected organizational personnel with incident handling responsibilities to determine what automated mechanisms are employed to support the incident handling process and how the mechanisms improve the process.*

Applicability: Moderate and High impact levels

*IR-4.7. **Examine** organizational documentation to determine if the automated mechanisms supporting the incident handling process are employed as defined in the incident response policy and procedures.*

Applicability: Moderate and High impact levels

*IR-4.8. **Test** selected incident handling mechanisms to determine if the mechanisms are operating as intended.*

Applicability: Moderate and High impact levels

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents on an ongoing basis.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Mechanisms, Activities

Assessment Procedure:

IR-5.1. ***Interview*** *selected organizational personnel with incident response responsibilities and* ***examine*** *organizational records to determine if the organization tracks and documents information system security incidents on an ongoing basis.*

Applicability: Moderate and High impact levels

IR-5.2. ***Examine*** *records of activity for (or actual organizational personnel engaged in) incident tracking to determine if the personnel are following designated procedures for conducting such activities.*

Applicability: Moderate and High impact levels

IR-5.3. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that incident monitoring for the information system is conducted correctly.*

Applicability: Moderate and High impact levels

IR-5.4. ***Interview*** *selected organizational personnel with incident response responsibilities and* ***examine*** *appropriate organizational records or documents to determine: (i) if information system security incidents are being monitored and documented consistently across the organization on an ongoing basis; and (ii) if anomalies or problems encountered during the incident monitoring process are being documented and the resulting information used to actively to improve the monitoring policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

IR-5.5. ***Interview*** *selected organizational personnel with incident response responsibilities to determine what automated mechanisms are employed to support security incident tracking and incident information collection and analysis, and how the mechanisms improve security incident tracking and incident information collection and analysis.*

Applicability: High impact level

IR-5.6. ***Examine*** *organizational records or documents to determine if the automated mechanisms supporting security incident tracking and incident information collection and analysis are employed as defined in the incident response policy and procedures.*

Applicability: High impact level

IR-5.7. ***Test*** *selected incident monitoring mechanisms to determine if the mechanisms are operating as intended.*

Applicability: Moderate and High impact levels

IR-6 INCIDENT REPORTING

Control: The organization promptly reports incident information to appropriate authorities.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*IR-6.1. **Interview** selected organizational personnel with incident response responsibilities and **examine** organizational records to determine if the organization promptly reports incident information to appropriate authorities.*

Applicability: All impact levels

*IR-6.2. **Examine** records of activity for (or actual organizational personnel engaged in) incident reporting to determine if personnel are following designated procedures for conducting such activities.*

Applicability: Moderate and High impact levels

*IR-6.3. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that incident reporting for the information system is conducted correctly.*

Applicability: Moderate and High impact levels

*IR-6.4. **Interview** selected organizational personnel with incident reporting responsibilities and **examine** appropriate organizational records or documents to determine: (i) if incident information is being reported promptly to appropriate authorities consistently across the organization on an ongoing basis; and (ii) if anomalies or problems encountered during incident reporting are being documented and the resulting information used to actively to improve the incident reporting policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization employs automated mechanisms to assist in the reporting of security incidents.

*IR-6.5. **Interview** selected organizational personnel with incident response responsibilities to determine what automated mechanisms are employed to support incident reporting and how the mechanisms improve the reporting process.*

Applicability: Moderate and High impact levels

*IR-6.6. **Examine** organizational records or documents to determine if the automated mechanisms supporting incident reporting are employed as defined in the incident response policy and procedures.*

Applicability: Moderate and High impact levels

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

Assessment Methods: Interview, Examine, Test

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*IR-7.1. **Examine** organizational records to determine if the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents.*

Applicability: All impact levels

*IR-7.2. **Test** the incident response support resource to determine if it provides the necessary advice and assistance to users of the information system for the handling and reporting of security incidents.*

Applicability: All impact levels

*IR-7.3. **Examine** records of activity for (or actual organizational personnel engaged in) the incident response support resource to determine if personnel are following designated procedures for conducting such activities.*

Applicability: Moderate and High impact levels

*IR-7.4. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that effective incident response support for the information system is provided.*

Applicability: Moderate and High impact levels

*IR-7.5. **Interview** selected organizational personnel with incident response responsibilities and **examine** appropriate organizational records or documents to determine: (i) if the incident response support resource is being consistently provided across the organization on an ongoing basis; and (ii) if anomalies or problems encountered during the provision of incident response support are being documented and the resulting information used to actively to improve the incident response support policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.

*IR-7.6. **Interview** selected organizational personnel with incident response responsibilities to determine what automated mechanisms are employed to increase the availability of incident response-related information and support and how the mechanisms improve the process.*

Applicability: Moderate and High impact levels

*IR-7.7. **Examine** organizational records or documents to determine if the automated mechanisms supporting the increased availability of incident response-related information and support are employed as defined in the incident response policy and procedures.*

Applicability: Moderate and High impact levels

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

[**Editor Note:** The security assessment procedures for this family are under development and will be included in subsequent drafts of Special Publication 800-53A.]

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

[**Editor Note:** The security assessment procedures for this family are under development and will be included in subsequent drafts of Special Publication 800-53A.]

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

[**Editor Note:** The security assessment procedures for this family are under development and will be included in subsequent drafts of Special Publication 800-53A.]

FAMILY: PLANNING **CLASS:** MANAGEMENT

[**Editor Note:** The security assessment procedures for this family are under development and will be included in subsequent drafts of Special Publication 800-53A.]

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

[**Editor Note:** The security assessment procedures for this family are under development and will be included in subsequent drafts of Special Publication 800-53A.]

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

[**Editor Note:** The security assessment procedures for this family are under development and will be included in subsequent drafts of Special Publication 800-53A.]

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

[**Editor Note:** The security assessment procedures for this family are under development and will be included in subsequent drafts of Special Publication 800-53A.]

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

[**Editor Note:** The security assessment procedures for this family are under development and will be included in subsequent drafts of Special Publication 800-53A.]

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

Background Information for Assessment*—The organization identifies and arranges access to: (i) elements of the organization responsible for developing, documenting, disseminating, reviewing, and updating system and information integrity policies and associated procedures for implementing the policies; (ii) the system and information integrity policies for the information system and any associated system and information integrity-related procedures; (iii) individuals or groups responsible for the implementation and operation system and information integrity procedures; (iv) any materials (e.g., security plans, records, schedules, assessment reports, after action reports, agreements, accreditation packages) associated with system and information integrity procedures and operations; and (v) guidance on the number/percentage of objects to be assessed by type.*

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

SI-1.1. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if system and information integrity policy and procedures: (i) exist; (ii) are documented; (iii) are disseminated to appropriate elements within the organization; (iv) are periodically reviewed by responsible parties within the organization; and (v) are updated, when organizational review indicates updates are required.*

Applicability: All impact levels

SI-1.2. ***Examine*** *the system and information integrity policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, and compliance for system and information integrity operations.*

Applicability: All impact levels

SI-1.3. ***Examine*** *the system and information integrity procedures to determine if the procedures are sufficient to address all areas identified in the system and information integrity policy and all associated system and information integrity controls.*

Applicability: All impact levels

SI-1.4. ***Examine*** *the system and information integrity policy and procedures to determine if the policy and procedures are updated periodically, when organizational reviews indicate updates are required.*

Applicability: Moderate and High impact levels

SI-1.5. ***Examine*** *the system and information integrity policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance.*

Applicability: Moderate and High impact levels

SI-1.6. ***Examine*** *system and information integrity policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the policy and procedures are disseminated, periodically reviewed, and updated.*

Applicability: Moderate and High impact levels

SI-1.7. ***Interview*** *selected organizational personnel with system and information integrity responsibilities and* ***examine*** *organizational records or documents to determine if anomalies or problems discovered by the organization in the content or application of the system and information integrity policy and procedures are being documented and the resulting information used to actively improve the policy and procedures.*

Applicability: High impact level

SI-1.8. ***Interview*** *selected organizational personnel with system and information integrity responsibilities and* ***examine*** *organizational records or documents to determine: (i) if the system and information integrity policy and procedure dissemination, reviews, and updates are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the dissemination, reviews, and updates of the policy and procedures are being documented and the resulting information used to actively improve the dissemination, review, and update processes on a continuous basis.*

Applicability: High impact level

SI-2 FLAW REMEDIATION

Control: The organization identifies, reports, and corrects information system flaws.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

SI-2.1. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if the organization identifies information systems affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.*

Applicability: All impact levels

SI-2.2. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if the organization installs newly released security relevant patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures.*

Applicability: All impact levels

SI-2.3. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation.*

Applicability: All impact levels

SI-2.4. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if the organization conducts continuous security assessments to identify vulnerabilities in the information system within its operating environment.*

Applicability: All impact levels

SI-2.5. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures.*

Applicability: All impact levels

SI-2.6. ***Examine*** *information system flaw reports to determine if the organization captures all appropriate information pertaining to the discovered flaws, including the cause of the information system flaws, mitigation activities, and lessons learned to identify necessary improvements in the flaw remediation process.*

Applicability: Moderate and High impact levels

SI-2.7. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if the organization employs a centralized patch management program to assist system administrators in identifying, acquiring, testing, and deploying patches.*

Applicability: Moderate and High impact levels

SI-2.8. ***Examine*** *the information system with automated security tools to determine the effectiveness of the organization's flaw remediation capabilities.*

Applicability: Moderate and High impact levels

SI-2.9. ***Examine*** *a listing/log of recent security flaw remediation actions performed on the information system, and for an appropriately sized selection of actions, verify that the system has been modified to reflect the required flaw remediation.*

Applicability: Moderate and High impact levels

SI-2.10. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that flaw remediation for the information system is conducted correctly.*

Applicability: Moderate and High impact levels

SI-2.11. ***Interview*** *selected organizational personnel with system and information integrity responsibilities and* ***examine*** *organizational records or documents to determine: (i) if flaw remediation efforts are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during flaw remediation are being documented and the resulting information used to actively improve the flaw remediation policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization centrally manages the flaw remediation process and installs updates automatically without individual user intervention.

SI-2.12. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if the organization centrally manages the flaw remediation process for the information system.*

Applicability: Optional

SI-2.13. ***Interview*** *selected organizational personnel with system and information integrity responsibilities and* ***examine*** *organizational records or documents to determine if the organization installs information system software updates automatically.*

Applicability: Optional

SI-2.14. ***Examine*** *the application that performs automatic updates (or the documentation for the application) to the information system software to determine how frequently automatic updates occur.*

Applicability: Optional

Control Enhancement:

(2) The organization employs automated mechanisms to periodically and upon command determine the state of information system components with regard to flaw remediation.

SI-2.15. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if the organization employs automated mechanisms to determine the security posture of information systems.*

Applicability: Optional

SI-3 MALICIOUS CODE PROTECTION

Control: The information system implements malicious code protection that includes a capability for automatic updates.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

*SI-3.1. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs virus protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.*

Applicability: All impact levels

*SI-3.2. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses).*

Applicability: All impact levels

*SI-3.3. **Examine** virus protection mechanisms to determine if the mechanisms detect and eradicate malicious code transported: (i) by electronic mail, electronic mail attachments, Internet access, removable media (e.g., diskettes, or compact discs), or other common means; or (ii) by exploiting information system vulnerabilities.*

Applicability: All impact levels

*SI-3.4. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization updates virus protection mechanisms whenever new releases are available in accordance with organizational policy and procedures.*

Applicability: All impact levels

*SI-3.5. **Examine** virus protection mechanisms to determine if the mechanisms have been appropriately updated to include the latest virus definitions.*

Applicability: All impact levels

*SI-3.6. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs virus protection mechanisms for applications that may transfer malicious code (e.g., file transfer software, instant messaging software).*

Applicability: All impact levels

*SI-3.7. **Examine** virus protection mechanisms to determine if the mechanisms are configured to perform periodic scans of the information system as well as real-time scans of each file as it is downloaded, opened, or executed.*

Applicability: All impact levels

*SI-3.8. **Examine** virus protection mechanisms to determine if the mechanisms are configured to disinfect and quarantine infected files.*

Applicability: All impact levels

SI-3.9. ***Examine*** *electronic mail clients and servers to determine if the clients and servers and are configured to block attachments with file extensions associated with malicious code (e.g., .pif, .vbs), and suspicious file extension combinations (e.g., .txt.vbs, .htm.exe).*

Applicability: All impact levels

SI-3.10. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the information system is effectively protected from malicious code.*

Applicability: Moderate and High impact levels

SI-3.11. ***Interview*** *selected organizational personnel with system and information integrity responsibilities and* ***examine*** *organizational records or documents to determine: (i) if malicious code protection measures are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during malicious code protection are being documented and the resulting information used to actively improve malicious code protection policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization centrally manages virus protection mechanisms.

SI-3.12. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if the organization centrally manages virus protection mechanisms employed in organizational information systems.*

Applicability: Moderate and High impact levels

Control Enhancement:

(2) The information system automatically updates virus protection mechanisms.

SI-3.13. ***Examine*** *virus protection mechanisms to determine if the mechanisms are configured to download and install updates automatically directly from the vendor or some other trusted source.*

Applicability: High impact level

SI-4 INTRUSION DETECTION TOOLS AND TECHNIQUES

Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

*SI-4.1. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs intrusion detection tools and techniques to include: intrusion detection systems, virus protection software, log monitoring software, network forensic analysis tools.*

Applicability: Moderate and High impact levels

*SI-4.2. **Examine** intrusion detection tools to determine if the tools are configured to detect vulnerabilities, changes to the network, both known and unknown attack signatures, and traffic anomalies.*

Applicability: Moderate and High impact levels

*SI-4.3. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization is appropriately staffed and operational to monitor intrusion detection systems in accordance with organizational policy and procedures.*

Applicability: Moderate and High impact levels

*SI-4.4. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that intrusion detection tools and techniques are employed correctly within the information system.*

Applicability: Moderate and High impact levels

*SI-4.5. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine: (i) if intrusion detection tools and techniques are being consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the implementation of intrusion detection tools and techniques are being documented and the resulting information used to improve intrusion detection policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

The organization networks individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

*SI-4.6. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization employs a centrally managed, systemwide intrusion detection capability.*

Applicability: Optional

Control Enhancement:

The organization employs automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

*SI-4.7. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization is capable of immediately investigating, reporting, and responding to suspicious activity in real-time.*

Applicability: Optional

Control Enhancement:

The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

SI-4.8. ***Interview*** *selected organizational personnel with system and information integrity responsibilities and* ***examine*** *organizational records or documents to determine if the organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms.*

Applicability: Optional

Control Enhancement:

The information system monitors outbound communications for unusual or unauthorized activities indicating the presence of malware (e.g., malicious code, spyware, adware).

SI-4.9. ***Examine*** *organizational records or documents to determine if the information system monitors outbound communications for unusual or unauthorized activities indicating the presence of malware.*

Applicability: Optional

SI-4.10. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if information system monitoring logs are reviewed to assess if there is a pattern of unusual or unauthorized activities.*

Applicability: Optional

SI-5 SECURITY ALERTS AND ADVISORIES

Control: The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*SI-5.1. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization receives information system security alerts and advisories.*

Applicability: All impact levels

*SI-5.2. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization disseminates information system security alerts and advisories to appropriate personnel.*

Applicability: All impact levels

*SI-5.3. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization is capable of immediately reacting and responding to new security alerts and advisories.*

Applicability: All impact levels

*SI-5.4. **Examine** system documentation (including any logs documenting alerts/advisories) to determine if the organization is receiving security alerts/advisories and documenting the action that was taken to include the date/time of the action.*

Applicability: All impact levels

*SI-5.5. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that security alerts and advisories for the information system are effectively employed.*

Applicability: Moderate and High impact levels

*SI-5.6. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine: (i) if security alerts/advisories are being consistently received and responded to across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the implementation of security alerts/advisories are being documented and the resulting information used to actively improve the security alert/advisory policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancements:

(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

*SI-5.7. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if security alerts and advisories are automatically disseminated to the appropriate personnel throughout the organization.*

Applicability: Optional

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Control: The information system verifies the correct operation of security functions [*Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every* [*Assignment: organization-defined time-period*]] and [*Selection (one or more): notifies system administrator, shuts the system down, restarts the system*] when anomalies are discovered.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

SI-6.1. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if the information system verifies the correct operation of security functions upon system startup and restart, and/or upon command by users with appropriate privileges.*

Applicability: Moderate and High impact levels

SI-6.2. ***Interview*** *selected organizational personnel with system and information integrity responsibilities to determine if the information system notifies the system administrator, shuts the system down, or restarts the system when anomalies are discovered.*

Applicability: Moderate and High impact levels

SI-6.3. ***Examine*** *the system to determine if it verifies the correct operations of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered.*

Applicability: Moderate and High impact levels

SI-6.4. ***Examine*** *organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the verification of security functions within the information system is performed correctly.*

Applicability: Moderate and High impact levels

SI-6.5. ***Interview*** *selected organizational personnel with system and information integrity responsibilities and* ***examine*** *organizational records or documents to determine: (i) if security functionality verification is consistently performed across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during security functionality verification are being documented and the resulting information used to actively improve the security functionality verification policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization employs automated mechanisms to provide notification of failed security tests.

SI-6.6. ***Interview*** *selected organizational personnel with system and information integrity responsibilities and* ***examine*** *organizational records or documents to determine if the organization employs automated mechanisms to provide notification of failed security tests.*

Applicability: High impact level

SI-6.7. ***Examine*** *information system output to verify that failed security test results are provided to the appropriate organizational personnel.*

Applicability: High impact level

Control Enhancement:

(2) The organization employs automated mechanisms to support management of distributed security testing.

SI-6.8. ***Interview*** *selected organizational personnel with system and information integrity responsibilities and* ***examine*** *organizational records or documents to determine if the organization employs automated mechanisms to support management of distributed security testing.*

Applicability: Optional

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Control: The information system detects and protects against unauthorized changes to software and information.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Activities

Assessment Procedure:

*SI-7.1. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs integrity verification software on the information system to look for evidence of information tampering, errors, and omissions.*

Applicability: High impact level

*SI-7.2. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes).*

Applicability: High impact level

*SI-7.3. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs tools to automatically monitor the integrity of the information system and the applications the system hosts.*

Applicability: High impact level

*SI-7.4. **Examine** information system integrity applications and tools to determine if the applications and tools effectively detect unauthorized changes to software and information.*

Applicability: High impact level

*SI-7.5. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the information system correctly detects and protects against unauthorized changes to software and information.*

Applicability: High impact level

*SI-7.6. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine: (i) if the information system detects and protects against unauthorized changes to software and information consistently and on an ongoing basis; and (ii) if anomalies or problems encountered during the detection of and protection against unauthorized changes to software and information are being documented and the resulting information used to actively improve the detection and protection policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

SI-8 SPAM AND SPYWARE PROTECTION

Control: The information system implements spam and spyware protection.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

*SI-8.1. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs spam and spyware protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.*

Applicability: Moderate and High impact levels

*SI-8.2. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet access, removable media (e.g., diskettes or compact disks), or other common means.*

Applicability: Moderate and High impact levels

*SI-8.3. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization updates spam and spyware protection mechanisms whenever new releases are available in accordance with organizational policy and procedures.*

Applicability: Moderate and High impact levels

*SI-8.4. **Examine** spam and spyware mechanisms and organizational records or documents to determine if the mechanisms have been appropriately updated with the most current versions.*

Applicability: Moderate and High impact levels

*SI-8.5. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the information system correctly protects against spam and spyware.*

Applicability: Moderate and High impact levels

*SI-8.6. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine: (i) if spam and spyware protection are consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during the implementation of spam and spyware protection are being documented and the resulting information used to actively improve the spam and spyware protection policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

Control Enhancement:

(1) The organization centrally manages spam and spyware protection mechanisms.

*SI-8.7. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the organization employs a centralized management architecture to manage virus protection mechanisms for the information system.*

Applicability: High impact level

Control Enhancement:

(2) The information system automatically updates spam and spyware protection mechanisms.

SI-8.8. ***Examine*** *virus protection mechanisms to determine if the mechanisms are configured to download and install updates automatically from the vendor or some other trusted source.*

Applicability: Optional

SI-9 INFORMATION INPUT RESTRICTIONS

Control: The organization restricts the information input to the information system to authorized personnel only.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

*SI-9.1. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the information system employs restrictions (beyond typical access control) on personnel authorized to input information to the information system to include limitations based on specific operational/project responsibilities.*

Applicability: Moderate and High impact levels

*SI-9.2. **Examine** the information system to verify that user accounts are restricted from inputting information beyond the typical access controls unless specifically authorized based on operational/project responsibilities.*

Applicability: Moderate and High impact levels

*SI-9.3. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the information system correctly restricts inputs.*

Applicability: Moderate and High impact levels

*SI-9.4. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine: (i) if the organization restricts information systems inputs consistently across the information system and ongoing basis; and (ii) if anomalies or problems encountered during information system input operations are being documented and the resulting information used to actively improve the information system input policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

SI-10 INFORMATION INPUT ACCURACY, COMPLETENESS, AND VALIDITY

Control: The information system checks information inputs for accuracy, completeness, and validity.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications, Mechanisms

Assessment Procedure:

*SI-10.1. **Examine** the information system to determine if the system checks information inputs for accuracy, completeness, and validity of information as close to the point of origin as possible.*

Applicability: Moderate and High impact levels

*SI-10.2. **Examine** the information system to determine if the system employs rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) to ensure that inputs match specified definitions for format and content.*

Applicability: Moderate and High impact levels

*SI-10.3. **Examine** the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands.*

Applicability: Moderate and High impact levels

*SI-10.4. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the information system correctly checks information input accuracy, completeness, and validity.*

Applicability: Moderate and High impact levels

*SI-10.5. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine: (i) if information input accuracy, completeness, and validity checks are consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during information input checks are being documented and the resulting information used to actively improve the information input checking policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

SI-11 ERROR HANDLING

Control: The information system identifies and handles error conditions in an expeditious manner.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*SI-11.1. **Examine** the information system to determine if the system identifies and handles error conditions in an expeditious manner.*

Applicability: Moderate and High impact levels

*SI-11.2. **Examine** the information system to determine if the system provides timely user error messages that contain useful information to users without revealing information that could be exploited by adversaries.*

Applicability: Moderate and High impact levels

*SI-11.3. **Examine** the information system to determine if the system provides error messages only to authorized personnel (e.g., system administrators, maintenance personnel).*

Applicability: Moderate and High impact levels

*SI-11.4. **Examine** the information system to determine if the system does not list sensitive information (e.g., account numbers, social security numbers, and credit card numbers) in error logs or associated administrative messages.*

Applicability: Moderate and High impact levels

*SI-11.5. **Interview** selected organizational personnel with system and information integrity responsibilities to determine if the information system is able to identify and handle error conditions in compliance with organizational policy and procedures.*

Applicability: Moderate and High impact levels

*SI-11.6. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that the information system correctly handles errors.*

Applicability: Moderate and High impact levels

*SI-11.7. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine: (i) if error handling actions are consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during error handling are being documented and the resulting information used to actively improve the error handling policy, procedures, and processes on a continuous basis.*

Applicability: High impact level

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Control: The organization handles and retains output from the information system in accordance with organizational policy and operational requirements.

Assessment Methods: Interview, Examine

Assessment Objects: Individuals, Specifications

Assessment Procedure:

*SI-12.1. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization retains output from the information system in accordance with organizational policy and operational requirements/procedures.*

Applicability: Moderate and High impact levels

*SI-12.2. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine if the organization handles output from the information system in accordance with: (i) labeled or marked instructions on information system output (including paper and digital media) that includes, but not limited to, special instructions for dissemination, distribution, transport, or storage of information system output; and (ii) organizational policy and operational requirements/procedures..*

Applicability: Moderate and High impact levels

*SI-12.3. **Examine** organizational policy and procedures to determine if specific parties are assigned responsibility and specific actions are defined to ensure that information output handling and retention are correctly implemented within the information system.*

Applicability: Moderate and High impact levels

*SI-12.4. **Interview** selected organizational personnel with system and information integrity responsibilities and **examine** organizational records or documents to determine: (i) if information output handling and retention are consistently applied across the information system on an ongoing basis; and (ii) if anomalies or problems encountered during information output handling and retention are being documented and the resulting information used to actively improve the information output handling and retention policy, procedures and processes on a continuous basis.*

Applicability: High impact level

APPENDIX G

ORGANIZING ASSESSMENT PROCEDURES

A WORKED EXAMPLE FOR EFFECTIVE ORGANIZATION OF ASSESSMENT PROCEDURES

This appendix provides a worked example for organizing the assessment procedures in the master catalog (Appendix F) by information system impact level and by assessment method. The identifier in brackets (e.g., [CP-5]) following each procedural statement corresponds to the assessment procedure identifier in Appendix F indicating the source from which the procedural statement was obtained. The contingency planning family of assessment procedures is used to demonstrate how the assessment procedures may be organized to create a more effective security assessment plan. It should be noted that during the tailoring process of the initial security control baselines as described in NIST Special Publication 800-53, organizations may have developed and implemented additional security controls for their information systems that are not included in this special publication. The organization may have also applied the scoping guidance from NIST Special Publication 800-53 to eliminate or downgrade selected security controls or employed compensating controls. In the above situations, the set of assessment procedures should be modified accordingly.

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

LOW IMPACT INFORMATION SYSTEMS

ASSESSMENT METHOD: Interview

CP-1, CP-2, CP-5

Interview *selected organizational personnel with contingency planning and plan implementation responsibilities to determine—*

(i) if contingency planning policy and procedures:

- *exist;* [CP-1.1]
- *are documented;* [CP-1.1]
- *are disseminated to appropriate elements within the organization;* [CP-1.1]
- *are periodically reviewed by responsible parties within the organization;* [CP-1.1]
- *are updated when organizational review indicates updates are required.* [CP-1.1]

(ii) if a contingency plan:

- *exists;* [CP-2.1]
- *is disseminated to appropriate elements and organizational personnel within the organization;* [CP-2.1]
- *is reviewed and approved by responsible officials within the organization;* [CP-2.1]
- *is updated in accordance with organization defined frequency (at least annually).* [CP-5.1]

(iii) if needed changes are reflected in the contingency plan. [CP-5.2]

CP-9

Interview *organizational personnel responsible for information system backup to determine if the user-level and system-level information (including system state information) that is required to be backed up is defined and the location for storing backup information is identified.* [CP-9.1]

CP-10

Interview *organizational personnel responsible for employing mechanisms to recover and reconstitute the information system to its original state to determine if mechanisms and procedures are available and are being applied.* [CP-10.1]

ASSESSMENT METHOD: Examine

CP-1, CP-2, CP-5

Examine *the contingency planning policy, the contingency plan procedures, and the contingency plan to determine:*

(i) if the policy addresses purpose, scope, roles, responsibilities, and compliance for contingency operations; [CP-2.1]

(ii) if the procedures are sufficient to address all areas identified in the contingency planning policy and all associated contingency planning controls; [CP-2.3]

(iii) if the content of the plan is consistent with NIST Special Publication 800-34 and addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system; [CP-2.2]

(iv) if revisions to the plan reflect the needed changes based on the organization's experiences during plan implementation, execution, and testing. [CP-5.3]

Examine *records of information system/organizational changes or problems encountered during contingency plan implementation, execution, or testing to determine if needed changes are reflected in the contingency plan.* [CP-5.2]

CP-9

Examine *information system backup procedures and selected information backup media (or selected records of such back up if available) to determine:*

(i) if procedures are defined for backing up required user-level and system-level information (including system state information) within organization-defined frequency, and storing backup information in a secure location; [CP-9.2]

(ii) if the required user-level and system-level information is backed up within the organization-defined frequency and stored in the designated location in accordance with information system backup procedures. [CP-9.3]

CP-10

Examine *information system recovery and reconstitution procedures to determine:*

(i) if means are identified for capturing the system's operation state including all system parameters, patches, configuration settings and application and system software prior to information system disruption or failure; [CP-10.2]

(ii) if the procedures require the system be tested upon information system recovery and reconstitution. [CP-10.3]

ASSESSMENT METHOD: Test

CP-10

Test *information system recovery and reconstitution mechanisms using selected components of the information system operations to determine if the system can be fully restored to its original operational state.* [CP-10.4]

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

MODERATE IMPACT INFORMATION SYSTEMS

ASSESSMENT METHOD: Interview

CP-1, CP-2, CP-5

Interview *selected organizational personnel with contingency planning and plan implementation responsibilities to determine—*

(i) if contingency planning policy and procedures:

- *exist;* [CP-1.1]
- *are documented;* [CP-1.1]
- *are disseminated to appropriate elements within the organization;* [CP-1.1]
- *are periodically reviewed by responsible parties within the organization;* [CP-1.1]
- *are updated when organizational review indicates updates are required.* [CP-1.1]

(ii) if a contingency plan:

- *exists;* [CP-2.1]
- *is disseminated to appropriate elements and organizational personnel within the organization;* [CP-2.1]
- *is reviewed and approved by responsible officials within the organization;* [CP-2.1]
- *is updated in accordance with organization defined frequency (at least annually);* [CP-5.1]
- *is consistent with the organization's contingency planning policy and procedures.* [CP-2.3]

(iii) if needed changes are reflected in the contingency plan; [CP-5.2]

(iv) if key operating elements within the organization are ready to implement the contingency plan; [CP-2.1]

(v) if contingency plan development is coordinated with other organizational elements responsible for related plans identified by the organization; [CP-2.7]

(vi) if contingency plan development is coordinated with the related plans and the contingency plan supports the requirements in the related plans. [CP-2.8]

CP-4

Interview *selected organizational personnel with contingency plan and plan implementation responsibilities to determine:*

(i) the overall effectiveness of the contingency plan and the readiness of the organization to execute the plan; [CP-4.3]

(ii) if the contingency plan test results are being reviewed and if corrective actions are being taken; [CP-4.4]

(iii) if contingency plan testing is coordinated with other organizational elements responsible for related plans identified by the organization and is coordinated with the testing associated with the related plans. [CP-4.7 and CP-4.8]

CP-6

Interview *alternate storage site administrators to determine if alternate storage site agreements are currently in place.* [CP-6.1]

CP-7

Interview *alternate processing site administrators to determine if agreements are currently in place to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.* [CP-7.1]

CP-8

Interview *primary and alternate telecommunication service administrators to determine:*

(i) if agreements are currently in place to permit the resumption of telecommunication services for critical mission/business functions within organization-defined time period when the primary telecommunications capabilities are unavailable; [CP-8.1]

(ii) if agreements contain priority of service provisions in accordance with the availability requirements defined in the organization's contingency plan; [CP-8.4]

(iii) if the alternate telecommunication services share a single point of failure with the primary telecommunications services. [CP-8.5]

CP-9

Interview *organizational personnel responsible for information system backup to determine if the user-level and system-level information (including system state information) that is required to be backed up is defined and the location for storing backup information is identified.* [CP-9.1]

CP-10

Interview *organizational personnel responsible for employing mechanisms to recover and reconstitute the information system to its original state to determine if mechanisms and procedures are available and are being applied.* [CP-10.1]

ASSESSMENT METHOD: Examine

CP-1, CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, CP-8, CP-9, CP-10

Examine *the contingency planning policy, the contingency plan procedures, other organizational procedures, and the contingency plan to determine:*

(i) if the policy addresses purpose, scope, roles, responsibilities, and compliance for contingency operations; [CP-2.1]

(ii) if the procedures are sufficient to address all areas identified in the contingency planning policy and all associated contingency planning controls; [CP-2.3]

(iii) if the policy and procedures are updated periodically, when organizational reviews indicate updates are required; [CP-1.4]

(iv) if the policy is consistent with the organization's mission and functions and associated laws, directives, policies, regulations, standards, and guidance. [CP-1.5]

(v) if specific parties are assigned responsibility and specific actions are defined to ensure that:

- *the contingency planning policy and procedures are disseminated, periodically reviewed, and updated;* [CP-1.6]
- *the contingency plan is correctly implemented and meets its required function and purpose;* [CP-2.5]
- *contingency plan reviews and updates are conducted correctly;* [CP-5.4]
- *contingency training is conducted correctly;* [CP-3.3]
- *contingency plan testing is conducted correctly;* [CP-4.5]
- *necessary alternate storage site agreements are correctly initiated to permit information system backup operations;* [CP-6.3]
- *necessary alternate processing site agreements are correctly initiated to permit the resumption of information system operations for critical mission/business functions within an organization-defined time period;* [CP-7.3]
- *necessary alternate telecommunications service agreements are correctly initiated to permit the resumption of information system operations for critical mission/business functions within an organization-defined time period;* [CP-8.2]
- *information system backups are conducted correctly;* [CP-9.4]
- *information system recovery and reconstitution are conducted correctly.* [CP-10.5]

(vi) if the content of the contingency plan is consistent with NIST Special Publication 800-34 and addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system; [CP-2.2]

(vii) if revisions to the plan reflect the needed changes based on the organization's experiences during plan implementation, execution, and testing. [CP-5.3]

CP-3

Examine *organizational records to determine:*

(i) if contingency training is provided to individuals implementing the contingency plan; [CP-3.1]

(ii) if records include the type of contingency training received and the date completed; [CP-3.1]

(iii) if initial and refresher training of individual roles and responsibilities is provided in accordance with organization-defined frequency, at least annually. [CP-3.1]

Examine *training material for selected contingency roles and responsibilities to determine if the training material addresses the procedures/activities for implementing those roles and responsibilities.* [CP-3.2]

CP-4

Examine *organizational records or documents to determine:*

(i) if the organization tests its contingency plan in accordance with organization-defined frequency, at least annually, and the results of the tests are documented; [CP-4.1]

(ii) if the contingency plan tests (or exercises) address key aspects of the plan and if the tests (or exercises) confirm that the plan objectives are met; [CP-4.1]

(iii) if the contingency plan test results are being reviewed and if corrective actions are being taken; [CP-4.4]

(iv) the overall effectiveness of the contingency plan and the readiness of the organization to execute the plan. [CP-4.3]

CP-5

Examine *records of information system/organizational changes or problems encountered during contingency plan implementation, execution, or testing to determine if needed changes are reflected in the contingency plan.* [CP-5.3]

CP-6

Examine *alternate storage site agreements to determine if agreements are currently in place.* [CP-6.1]

Examine *each alternate storage site to determine:*

(i) if the site is available and accessible in accordance with the alternate site agreement; [CP-6.2]

(ii) if the site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary storage site. [CP-6.6]

Examine *the organization's contingency plan to determine if the plan identifies the primary storage site hazards.* [CP-6.5]

CP-7

Examine *alternate processing site agreements to determine if agreements are currently in place to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.* [CP-7.1]

Examine *each alternate processing site to determine:*

(i) if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period; [CP-7.2]

(ii) if the site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary processing site. [CP-7.6]

Examine *the organization's contingency plan to determine if the plan identifies the primary processing site hazards.* [CP-7.5]

CP-8

Examine *alternate telecommunication service agreements to determine:*

(i) if agreements are currently in place to permit the resumption of telecommunication service operations for critical mission/business functions within organization-defined time period when the primary telecommunications capabilities are unavailable; [CP-8.1]

(ii) if agreements contain priority of service provisions in accordance with the availability requirements defined in the organization's contingency plan; [CP-8.4]

(iii) if the alternate telecommunication services share a single point of failure with the primary telecommunications services. [CP-8.5]

CP-9

Examine *information system backup procedures and selected information backup media (or selected records of such back up if available) to determine:*

(i) if procedures are defined for backing up required user-level and system-level information (including system state information) within organization-defined frequency, and storing backup information in a secure location; [CP-9.2]

(ii) if the required user-level and system-level information is backed up within the organization-defined frequency and stored in the designated location in accordance with information system backup procedures. [CP-9.3]

Examine *test results from organization testing of backup information to determine if testing is conducted within the organization-defined frequency, and testing results indicate backup media reliability and information integrity.* [CP-9.6]

CP-10

Examine *information system recovery and reconstitution procedures to determine:*

(i) if means are identified for capturing the system's operation state including all system parameters, patches, configuration settings and application and system software prior to information system disruption or failure; [CP-10.2]

(ii) if the procedures require the system be tested upon information system recovery and reconstitution. [CP-10.3]

ASSESSMENT METHOD: Test

CP-10

Test *information system recovery and reconstitution mechanisms using selected components of the information system operations to determine if the system can be fully restored to its original operational state.* [CP-10.4]

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

HIGH IMPACT INFORMATION SYSTEMS

ASSESSMENT METHOD: Interview

CP-1, CP-2, CP-5

Interview *selected organizational personnel with contingency planning and plan implementation responsibilities to determine—*

(i) if contingency planning policy and procedures:

- *exist;* [CP-1.1]
- *are documented;* [CP-1.1]
- *are disseminated to appropriate elements within the organization;* [CP-1.1]
- *are periodically reviewed by responsible parties within the organization;* [CP-1.1]
- *are updated when organizational review indicates updates are required.* [CP-1.1]

(ii) if a contingency plan:

- *exists;* [CP-2.1]
- *is disseminated to appropriate elements and organizational personnel within the organization;* [CP-2.1]
- *is reviewed and approved by responsible officials within the organization;* [CP-2.1]
- *is updated in accordance with organization defined frequency (at least annually);* [CP-5.1]
- *is consistent with the organization's contingency planning policy and procedures.* [CP-2.3]

(iii) if needed changes are reflected in the contingency plan; [CP-5.2]

(iv) if key operating elements within the organization are ready to implement the contingency plan; [CP-2.1]

(v) if contingency plan development is coordinated with other organizational elements responsible for related plans identified by the organization; [CP-2.7]

(vi) if the contingency plan is being consistently reviewed and updated on an ongoing basis; [CP-5.5]

(vii) if contingency plan development is coordinated with the related plans and the contingency plan supports the requirements in the related plans; [CP-2.8]

(viii) if anomalies or problems encountered during the dissemination, reviews, and updates of the policy and procedures are being documented and the resulting information used to actively improve the dissemination, review, and update processes on a continuous basis; [CP-1.8]

(ix) if anomalies or problems encountered during the implementation of the contingency plan or plan update are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with the plan or plan update on a continuous basis; [CP-2.6 and CP-5.5]

(x) if anomalies or problems discovered by the organization in the content or application of the contingency planning policy and procedures are being documented and the resulting information used to actively improve the policy and procedures. [CP-1.7]

(xi) if the contingency planning policy and procedure dissemination, reviews, and updates, and the contingency plan are being consistently applied across the information system on an ongoing basis. [CP-1.8]

CP-3

Interview *selected organizational personnel with contingency planning and plan implementation responsibilities to determine:*

(i) if contingency training is being consistently conducted across the organization on an ongoing basis; [CP-3.4]

(ii) if anomalies or problems encountered during contingency training are being documented and the resulting information used to actively improve the training policy, procedures, and processes on a continuous basis; [CP-3.4]

(iii) what contingency training events are simulated and how these events improve the training process. [CP-3.5]

CP-4

Interview *selected organizational personnel with contingency plan and plan implementation responsibilities to determine:*

(i) the overall effectiveness of the contingency plan and the readiness of the organization to execute the plan; [CP-4.3]

(ii) if the contingency plan test results are being reviewed and if corrective actions are being taken; [CP-4.4]

(iii) if contingency plan testing is coordinated with other organizational elements responsible for related plans identified by the organization and is coordinated with the testing associated with the related plans; [CP-4.7 and CP-4.8]

(iv) if contingency plan testing is being consistently conducted across the organization on an ongoing basis; [CP-4.6]

(v) if anomalies or problems encountered during contingency plan testing are being documented and the resulting information used to actively improve the testing policy, procedures, and processes on a continuous basis; [CP-4.6]

(vi) if the personnel are familiar with the alternate processing site and the capabilities available at the site. [CP-4.9]

CP-6

Interview *alternate storage site administrators to determine;*

(i) if alternate storage site agreements are currently in place; [CP-6.1]

(ii) if alternate storage site agreements are being consistently reviewed on an ongoing basis; [CP-6.4]

(iii) if anomalies or problems encountered during the development or review of alternate storage site agreements are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with the development or review of alternate storage site agreements on a continuous basis. [CP-6.4]

CP-7

Interview *alternate processing site administrators to determine:*

(i) *if agreements are currently in place to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.* [CP-7.1]

(ii) *if agreements are currently in place and contain priority of service provisions in accordance with the organization's availability requirements.* [CP-7.9]

Interview *selected organizational personnel with contingency planning and plan implementation responsibilities to determine:*

(i) if alternate processing site agreements are being consistently reviewed on an ongoing basis; [CP-7.4]

(ii) if anomalies or problems encountered during the development or review of alternate processing site agreements are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with the development or review of alternate processing site agreements on a continuous basis. [CP-7.4]

CP-8

Interview *primary and alternate telecommunication service administrators to determine:*

(i) if agreements are currently in place to permit the resumption of telecommunication services for critical mission/business functions within organization-defined time period when the primary telecommunications capabilities are unavailable; [CP-8.1]

(ii) if agreements contain priority of service provisions in accordance with the availability requirements defined in the organization's contingency plan; [CP-8.4]

(iii) if the alternate telecommunication services share a single point of failure with the primary telecommunications services; [CP-8.5]

(iv) if the contingency plans are adequate. [CP-8.7]

Interview *selected organizational personnel with contingency planning and plan implementation responsibilities to determine:*

(i) if primary and alternate telecommunications service agreements are being consistently reviewed on an ongoing basis; [CP-8.2]

(ii) if anomalies or problems encountered during the development or review of primary and alternate telecommunications service agreements are being documented and the resulting information used to actively improve the policy, procedures, and processes associated with the development or review of primary and alternate telecommunications service agreements on a continuous basis. [CP-8.3]

CP-9

Interview *organizational personnel responsible for information system backup to determine if the user-level and system-level information (including system state information) that is required to be backed up is defined and the location for storing backup information is identified.* [CP-9.1]

Interview *selected organizational personnel with contingency planning and plan implementation responsibilities to determine:*

(i) if information system backups are being consistently conducted across the information system on an ongoing basis; [CP-9.5]

(ii) if anomalies or problems encountered during information system backup operations are being documented and the resulting information used to actively improve the system backup policy, procedures, and processes on a continuous basis. [CP-9.5]

CP-10

Interview *organizational personnel responsible for employing mechanisms to recover and reconstitute the information system to its original state to determine if mechanisms and procedures are available and are being applied.* [CP-10.1]

Interview *selected organizational personnel with contingency planning and plan implementation responsibilities to determine:*

(i) if recovery and reconstitution operations are being consistently conducted across the information system on an ongoing basis; [CP-10.6]

(ii) if anomalies or problems encountered during information system recovery and reconstitution are being documented and the resulting information used to actively improve the recovery and reconstitution policy, procedures, and processes on a continuous basis. [CP-10.6]

ASSESSMENT METHOD: Examine

CP-1, CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, CP-8, CP-9, CP-10

Examine *the contingency planning policy, the contingency plan procedures, other organizational procedures, and the contingency plan to determine:*

(i) if the policy addresses purpose, scope, roles, responsibilities, and compliance for contingency operations; [CP-2.1]

(ii) if the procedures are sufficient to address all areas identified in the contingency planning policy and all associated contingency planning controls; [CP-2.3]

(iii) if the policy and procedures are updated periodically, when organizational reviews indicate updates are required; [CP-1.4]

(iv) if the policy is consistent with the organization's mission and functions and associated laws, directives, policies, regulations, standards, and guidance. [CP-1.5]

(v) if specific parties are assigned responsibility and specific actions are defined to ensure that:

- *the contingency planning policy and procedures are disseminated, periodically reviewed, and updated;* [CP-1.6]
- *the contingency plan is correctly implemented and meets its required function and purpose;* [CP-2.5]
- *contingency plan reviews and updates are conducted correctly;* [CP-5.4]
- *contingency training is conducted correctly;* [CP-3.3]
- *contingency plan testing is conducted correctly;* [CP-4.5]
- *necessary alternate storage site agreements are correctly initiated to permit information system backup operations;* [CP-6.3]
- *necessary alternate processing site agreements are correctly initiated to permit the resumption of information system operations for critical mission/business functions within an organization-defined time period;* [CP-7.3]
- *necessary alternate telecommunications service agreements are correctly initiated to permit the resumption of information system operations for critical mission/business functions within an organization-defined time period;* [CP-8.2]
- *information system backups are conducted correctly;* [CP-9.4]
- *information system recovery and reconstitution are conducted correctly.* [CP-10.5]

(vi) if the content of the contingency plan is consistent with NIST Special Publication 800-34 and addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system; [CP-2.2]

(vii) if revisions to the plan reflect the needed changes based on the organization's experiences during plan implementation, execution, and testing. [CP-5.2]

Examine *organizational records or documents to determine:*

(i) if anomalies or problems discovered by the organization in the content or application of the contingency planning policy and procedures are being documented and the resulting information used to actively improve the policy and procedures; [CP-1.7]

(ii) if anomalies or problems encountered during the dissemination, reviews, and updates of the policy and procedures are being documented and the resulting information used to actively improve the dissemination, review, and update processes on a continuous basis; [CP-1.8]

(iii) if the contingency planning policy and procedure dissemination, reviews, and updates are being consistently applied across the information system on an ongoing basis; [CP-1.8]

(iv) if anomalies or problems encountered during the implementation of the contingency plan or the plan update process are being documented and the resulting information used to actively improve the plan on a continuous basis; [CP-2.6 and CP-5.5]

(v) if the contingency plan is being consistently applied across the information system on an ongoing basis; [CP-2.6]

(vi) if the contingency plan is being consistently reviewed and updated on an ongoing basis. [CP-5.5]

***Examine** records of information system/organizational changes or problems encountered during contingency plan implementation, execution, or testing to determine if needed changes are reflected in the contingency plan.* [CP-5.3]

CP-3

***Examine** organizational records and documentation to determine:*

(i) if contingency training is provided to individuals implementing the contingency plan; [CP-3.1]

(ii) if records include the type of contingency training received and the date completed; [CP-3.1]

(iii) if initial and refresher training of individual roles and responsibilities is provided in accordance with organization-defined frequency, at least annually; [CP-3.1]

(iv) if the contingency training is being consistently conducted across the organization on an ongoing basis; [CP-3.4]

(v) if anomalies or problems encountered during contingency training are being documented and the resulting information used to actively improve the training on a continuous basis. [CP-3.4]

***Examine** training material for selected contingency roles and responsibilities to determine if the training material addresses the procedures/activities for implementing those roles and responsibilities.* [CP-3.2]

***Examine** contingency plan/procedures to determine:*

(i) what contingency training events are simulated and how these events improve the training process; [CP-3.5]

(ii) if the simulated events identified by the organization are being employed in accordance with contingency training plans/procedures. [CP-3.6]

CP-4

***Examine** organizational records or documents to determine:*

(i) if the organization tests its contingency plan in accordance with organization-defined frequency, at least annually, and the results of the tests are documented; [CP-4.1]

(ii) if the contingency plan tests (or exercises) address key aspects of the plan and if the tests (or exercises) confirm that the plan objectives are met; [CP-4.1]

(iii) if the contingency plan test results are being reviewed and if corrective actions are being taken; [CP-4.4]

(iv) the overall effectiveness of the contingency plan and the readiness of the organization to execute the plan; [CP-4.3]

(v) if the contingency plan testing is being consistently conducted across the organization on an ongoing basis; [CP-4.6]

(vi) if anomalies or problems encountered during contingency plan testing are being documented and the resulting information used to actively improve the testing on a continuous basis; [CP-4.6]

(vii) if contingency plan testing is being performed at the alternate processing site and if the site can successfully support contingency operations. [CP-4.10]

CP-5

Examine *records of information system/organizational changes or problems encountered during contingency plan implementation, execution, or testing to determine if needed changes are reflected in the contingency plan.* [CP-5.3]

CP-6

Examine *alternate storage site agreements to determine:*

(i) if agreements are currently in place; [CP-6.1]

(ii) if the agreements specify configuration requirements to facilitate timely and effective recovery of system backup information (i.e. meeting recovery time and recovery point objectives). [CP-6.7]

Examine *each alternate storage site to determine:*

(i) if the site is available and accessible in accordance with the alternate site agreement; [CP-6.2]

(ii) if the site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary storage site. [CP-6.6]

Examine *the organization's contingency plan to determine if the plan identifies the primary storage site hazards.* [CP-6.5]

Examine *organizational records or documents to determine:*

(i) if alternate storage site agreements are being consistently reviewed on an ongoing basis; [CP-6.4]

(ii) if anomalies or problems encountered during the review process are being documented and the resulting information used to actively improve the agreements on a continuous basis. [CP-6.4]

Examine *the organization's contingency plan to determine:*

(i) if the plan identifies the primary storage site hazards; [CP-6.5]

(ii) if the plan identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; [CP-6.9]

(iii) if the plan defines explicit mitigation actions for those accessibility problems. [CP-6.9]

CP-7

Examine *alternate processing site agreements to determine:*

(i) if agreements are currently in place to permit the resumption of information system operations for critical mission/business functions within organization-defined time period; [CP-7.1]

(ii) if agreements contain priority of service provisions in accordance with the organization's availability requirements; [CP-7.9]

(iii) if the agreements specify the configuration requirements needed to support the minimum required operational capability of the organization. [CP-7.10]

Examine *each alternate processing site to determine:*

(i) if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period; [CP-7.2]

(ii) if the site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary processing site. [CP-7.6]

Examine *the organization's contingency plan to determine:*

(i) if the plan identifies the primary processing site hazards; [CP-7.5]

(ii) if the plan identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; [CP-7.7]

(iii) if the plan defines explicit mitigation actions for those accessibility problems. [CP-7.7]

Examine *organizational records or documents to determine:*

(i) if alternate processing site agreements are being consistently reviewed on an ongoing basis; [CP-7.4]

(ii) if anomalies or problems encountered during the review process are being documented and the resulting information used to actively improve the agreements on a continuous basis. [CP-7.4]

CP-8

Examine *alternate telecommunication service agreements to determine:*

(i) if agreements are currently in place to permit the resumption of telecommunication service operations for critical mission/business functions within organization-defined time period when the primary telecommunications capabilities are unavailable; [CP-8.1]

(ii) if agreements contain priority of service provisions in accordance with the availability requirements defined in the organization's contingency plan; [CP-8.4]

(iii) if the alternate telecommunication services share a single point of failure with the primary telecommunications services. [CP-8.5]

Examine *organizational records or documents to determine:*

(i) if primary and alternate telecommunications service agreements are being consistently reviewed on an ongoing basis; [CP-8.3]

(ii) if anomalies or problems encountered during the review process are being documented and the resulting information used to actively improve the agreements on a continuous basis. [CP-8.3]

Examine *the alternate telecommunication service provider's site to determine if the site is sufficiently separated from the primary telecommunication service provider's site so as not to be susceptible to the same hazards identified at the primary telecommunication service provider's site.* [CP-8.6]

Examine *the contingency plans from the primary and alternate telecommunication service providers to determine if the contingency plans are adequate.* [CP-8.7]

CP-9

Examine *information system backup procedures and selected information backup media (or selected records of such back up if available) to determine:*

(i) if procedures are defined for backing up required user-level and system-level information (including system state information) within organization-defined frequency, and storing backup information in a secure location; [CP-9.2]

(ii) if the required user-level and system-level information is backed up within the organization-defined frequency and stored in the designated location in accordance with information system backup procedures. [CP-9.3]

Examine *test results from organization testing of backup information to determine if testing is conducted within the organization-defined frequency, and testing results indicate backup media reliability and information integrity.* [CP-9.6]

Examine *organizational records or documents to determine:*

(i) if information system backups are being consistently conducted across the information system on an ongoing basis; [CP-9.5]

(ii) if anomalies or problems encountered during information system backup operations are being documented and the resulting information used to actively improve the system backup process on a continuous basis; [CP-9.5]

(iii) if testing is conducted with selected backup information in the restoration of information system functions as part of contingency plan testing. [CP-9.7]

Examine *back up storage location to determine if back up copies of the operating system and other critical information system software are stored in a fire-rated container that is not collocated with the operational software.* [CP-9.8]

CP-10

Examine *information system recovery and reconstitution procedures to determine:*

(i) if means are identified for capturing the system's operation state including all system parameters, patches, configuration settings and application and system software prior to information system disruption or failure; [CP-10.2]

(ii) if the procedures require the system be tested upon information system recovery and reconstitution. [CP-10.3]

Examine *organizational records or documents to determine:*

(i) if recovery and reconstitution procedures are being consistently applied across the information system on an ongoing basis; [CP-10.6]

(ii) if anomalies or problems encountered during the information system recovery and reconstitution process are being documented and the resulting information used to actively improve the recovery and reconstitution process on a continuous basis. [CP-10.6]

Examine *test results or organizational records from contingency plan testing to determine if the organization includes a full recovery and reconstitution of the information system with the most recent backups as part of contingency plan testing.* [CP-10.7]

ASSESSMENT METHOD: Test

CP-3, CP-6, CP-7, CP-10

Test *selected contingency training simulated events to determine if organizational personnel respond as expected to the simulated crisis situation.* [CP-3.7]

Test *the alternate storage site operations to determine if the alternate site is configured to enable timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives) in accordance with the provisions of alternate storage site agreement.* [CP-6.8]

Test *the organization's mitigation actions for accessing the alternate storage site in the event of an area-wide disruption or disaster to determine if the mitigation actions resolve the associated accessibility problems.* [CP-6.10]

Test *the organization's mitigation actions for accessing the alternate processing site in the event of an area-wide disruption or disaster to determine if the mitigation actions resolve the associated accessibility problems.* [CP-7.8]

Test *selected components of the information system at the alternate processing site to determine if the site is configured to support the minimum required operational capability of the organization and is ready to use as the operational site.* [CP-7.11]

Test *information system recovery and reconstitution mechanisms using selected components of the information system operations to determine if the system can be fully restored to its original operational state.* [CP-10.4]