

NIST Special Publication 800-53A

Guide for Assessing the Security Controls in Federal Information Systems

NIST

**National Institute of
Standards and Technology**

Technology Administration
U.S. Department of Commerce

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

SECOND PUBLIC DRAFT

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

April 2006



U.S. Department of Commerce

Carlos M. Gutierrez, Secretary

Technology Administration

Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology

William Jeffrey, 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.

Draft

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 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.

NIST Special Publication 800-53A, 298 pages

(April 2006) CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There are references in this publication to documents currently under development by NIST in accordance with responsibilities assigned to NIST under the Federal Information Security Management Act of 2002. The methodologies in this document may be used even before the completion of such companion documents. Thus, until such time as each document is completed, current requirements, guidelines, and procedures (where they exist) remain operative. For planning and transition purposes, agencies may wish to closely follow the development of these new documents by NIST. Individuals are also encouraged to review the public draft documents and offer their comments to NIST. All NIST documents mentioned in this publication other than the ones noted above, are available at the Computer Security Division web site: <http://csrc.nist.gov/publications>.

THE PUBLIC COMMENT PERIOD FOR THIS DOCUMENT IS APRIL 21 THROUGH JULY 31, 2006.
COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY
LABORATORY, 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 and in particular, Elizabeth Chew, Mike Rohde, Bennett Hodge, Matthew Cho, Eric Hodge, Stacy Kendziorski, and Karen Ortiz, who reviewed drafts of this document and contributed to its development. A special note of thanks is also extended to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support. The authors also gratefully acknowledge and appreciate the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Draft

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

In accordance with the Federal Information Security Management Act of 2002, Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory, non-waiverable standard. To comply with the federal standard, agencies must first determine the security category of their information system in accordance with the provisions of FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and then apply the appropriate set of minimum (baseline) security controls in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. Agencies have flexibility in applying the minimum security controls based on the tailoring guidance provided in Special Publication 800-53. This allows agencies to adjust the security controls to more closely fit their mission requirements and operational environments.

If a NIST Special Publication is referenced in the Supplemental Guidance for a particular security control in Special Publication 800-53, agencies are required to follow that guidance when developing, implementing, and assessing that control. NIST guidance documents are traditionally written with a degree of flexibility in mind so that agencies can apply the basic concepts in the guidance while maintaining the needed flexibility for specific operational environments and unique conditions within their organizations. This is consistent with OMB policy as articulated in the annual FISMA Reporting Guidance.

The combination of FIPS 200 and NIST Special Publication 800-53 requires a foundational level of security for all federal information and information systems (other than national security-related) and establishes a level of “security due diligence” for federal agencies and their support contractors. The agency's risk assessment should validate the minimum security control set and determine if any additional controls are needed to protect the agency's operations and assets including mission, functions, image, or reputation.

See <http://csrc.nist.gov/sec-cert/ca-compliance.html> for additional information on compliance.

CAUTIONARY NOTES

Organizations should carefully consider the potential side effects of employing the methods and procedures defined in this special publication when assessing the security controls in *operational* information systems. Certain assessment methods and procedures, particularly those methods and procedures that directly impact the operation of hardware, software, and/or firmware components of an information system, may inadvertently affect the routine processing, transmission, and/or storage of information supporting critical and sensitive organizational missions. Organizations should take necessary precautions during security control assessment periods to ensure that organizational mission and functions continue to be supported by the information system.

The security controls referenced in this publication have been obtained from NIST Special Publication 800-53, Revision 1 (Public Draft), March 2006. Final publication of NIST Special Publication 800-53A is anticipated in December 2006. At that time, the security controls, control enhancements, and security control baselines will be updated to reflect the final publication of NIST Special Publication 800-53, Revision 1, targeted for release in July 2006.

Notes to Reviewers

NIST invites the public to review and comment upon this guideline. The second public draft of Special Publication 800-53A contains significant improvements in a variety of areas based on the feedback obtained from our customers during the initial public comment period. In addition to completing the remaining twelve families of assessment procedures for the security control families in NIST Special Publication 800-53, the following significant changes can be noted:

- Clarification of the purpose and target audience for the publication;
- Clarification of the purpose and use of the conceptual assessment framework;
- Refinement of assessment expectations;
- Reduction in the number of procedural steps for assessing security controls;
- Realignment of procedural steps within the security control assessment procedures;
- More user-friendly format for assessment procedures in the assessment procedure catalog;
- New summary table for minimum assessment procedures for security control baselines contained in NIST Special Publication 800-53; and
- Updates of supporting appendices.

We are once again, interested in your specific 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 information systems.

We are actively seeking to develop more effective delivery methods for our customers through database and web application tools which will greatly facilitate the application of this publication. The improved delivery vehicles for Special Publication 800-53A will be initiated after the completion of the second public draft of this publication. The most current information on this aspect of the project can be found on the FISMA Implementation Project web site.

Comments on this draft publication will be accepted through **July 31, 2006**. NIST will then revise the guideline and publish the final public draft by the end of October 2006. 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 agencies, their support contractors, 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.....	1
1.1	PURPOSE AND APPLICABILITY	1
1.2	TARGET AUDIENCE.....	2
1.3	SYSTEM DEVELOPMENT LIFE CYCLE	3
1.4	RELATIONSHIP TO OTHER ASSESSMENT PUBLICATIONS	3
1.5	REUSE OF ASSESSMENT RESULTS.....	4
1.6	ORGANIZATION OF THIS SPECIAL PUBLICATION.....	5
CHAPTER TWO	THE FUNDAMENTALS	6
2.1	FRAMEWORK FOR DEVELOPING ASSESSMENT PROCEDURES	6
2.2	DEFINING THE FRAMEWORK COMPONENTS	7
2.3	GENERATING ASSESSMENT PROCEDURES	9
2.4	CATALOGING ASSESSMENT PROCEDURES	10
CHAPTER THREE	THE PROCESS.....	12
3.1	BUILDING EFFECTIVE ASSURANCE ARGUMENTS	12
3.2	DEVELOPING SECURITY ASSESSMENT PLANS.....	13
3.3	DOCUMENTING AND ANALYZING ASSESSMENT RESULTS	16
3.4	CONTINUOUS MONITORING	17
3.5	APPLYING ASSESSMENT RESULTS	18
APPENDIX A	REFERENCES.....	19
APPENDIX B	GLOSSARY	23
APPENDIX C	ACRONYMS.....	33
APPENDIX D	ASSESSMENT METHOD DESCRIPTIONS	34
APPENDIX E	ASSESSMENT EXPECTATIONS	38
APPENDIX F	ASSESSMENT PROCEDURE CATALOG	41
	ACCESS CONTROL PROCEDURES	42
	AWARENESS AND TRAINING PROCEDURES	70
	AUDIT AND ACCOUNTABILITY PROCEDURES.....	75
	CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT PROCEDURES.....	90
	CONFIGURATION MANAGEMENT PROCEDURES	98
	CONTINGENCY PLANNING PROCEDURES	108
	IDENTIFICATION AND AUTHENTICATION PROCEDURES	125
	INCIDENT RESPONSE PROCEDURES.....	134
	MAINTENANCE PROCEDURES	142
	MEDIA PROTECTION PROCEDURES	151
	PHYSICAL AND ENVIRONMENTAL PROTECTION PROCEDURES	157
	PLANNING PROCEDURES	182
	PERSONNEL SECURITY PROCEDURES	188
	RISK ASSESSMENT PROCEDURES.....	196
	SYSTEM AND SERVICES ACQUISITION PROCEDURES	202
	SYSTEM AND COMMUNICATIONS PROTECTION PROCEDURES.....	216
	SYSTEM AND INFORMATION INTEGRITY PROCEDURES	243
APPENDIX G	ORGANIZING ASSESSMENT PROCEDURES	260
APPENDIX H	MINIMUM ASSESSMENT PROCEDURES – SUMMARY	277

CHAPTER ONE

INTRODUCTION

THE NEED TO ASSESS SECURITY CONTROL EFFECTIVENESS IN INFORMATION SYSTEMS

The selection and employment of appropriate *security controls* for an information system¹ are important tasks that can have major implications on the operations 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,² and availability of the system and its information.³ Once employed within an information system, security controls must be assessed to determine their overall effectiveness; that is, 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 control assessments play an important role in determining the overall security status of an information system and the ultimate risk to the operations and assets of the organization should that system be placed into operation or continued in its operation.

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 FISMA compliance.

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 3542.⁴ 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.

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 The FISMA definition of integrity includes non-repudiation and authenticity.

³ The complete definitions of management, operational, and technical controls can be found in Appendix B.

⁴ NIST Special Publication 800-59 provides guidance on identifying an information system as a national security system.

Organizations should use NIST Special Publication 800-53A to create a viable security assessment plan to determine the overall effectiveness of the security controls employed within an organizational information system. The assessment methods and procedures from Special Publication 800-53A represent a minimum level of security due diligence for organizations assessing the security controls in their information systems and should be used as a starting point for and as input to the security assessment plan. Organizations should supplement the assessment methods and procedures contained in this publication as needed, taking into consideration any platform-specific dependencies in the deployed hardware, software, or firmware that compose the information system. The selection of appropriate assessment methods and procedures for a particular information system depends on three factors:

- The security categorization of the information system in accordance with FIPS 199 and NIST Special Publication 800-53;
- The specific security controls selected and employed by the organization to protect the information system;⁵ and
- The level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system.

Risk assessments should also 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 NIST 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 policies and requirements, operational considerations, known threat and vulnerability information, and tolerance for risk to the organization's operations and assets.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse group of information system and information security professionals including: (i) individuals with information system and information security management and oversight responsibilities (e.g., authorizing officials, senior agency information security officers, information security managers); (ii) individuals with information system development responsibilities (e.g., program managers, systems integrators); (iii) individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, and information system security officers); and (iv) individuals with information system and information security assessment and monitoring responsibilities (e.g., system evaluators, certification agents and certification teams, independent verification and validation assessors).⁶ Commercial companies providing security control assessment, security certification, testing and evaluation, and/or auditing services can also benefit from the information in this publication.

⁵ The selection and employment of specific security controls for an information system includes the application of tailoring guidance from NIST Special Publication 800-53 to adjust the minimum security control baselines required by FIPS 200.

⁶ While the assessment methods and procedures contained in NIST Special Publication 800-53A can serve a diverse constituency, the primary focus of this publication is to support certification agents and certification teams conducting comprehensive assessments of the security controls in federal information systems and individuals responsible for the continuous monitoring of those controls as integral components of the security accreditation process.

1.3 SYSTEM DEVELOPMENT LIFE CYCLE

Security assessments should be conducted at various phases in the system development life cycle.⁷ NIST Special Publication 800-53A provides a comprehensive set of assessment methods and procedures to support the assessment activities that may be required for an information system during the system development life cycle. For example, security assessments should be initiated during the system development and acquisition phase of the life cycle by information system developers and by system integrators to ensure that the security controls required for the protection of the system are properly designed, developed, and implemented.⁸ This assessment process is sometimes referred to as developmental security testing and evaluation. Security assessments should also be conducted by information system owners, information system security officers, and independent certification agents during the system implementation phase and the operations and maintenance phase of the life cycle to ensure that the selected security controls are effective in the operational environment where the information system is deployed.⁹ Finally, at the end of the life cycle, security assessments should be conducted to ensure that important organizational information is purged from the information system prior to disposal. The results obtained from the security assessments will, in all likelihood, be used in different ways and for different purposes in creating sufficient evidence to give organizational officials confidence, or assurance, that the information system has adequate security to protect the operations and assets of the organization.

1.4 RELATIONSHIP TO OTHER ASSESSMENT 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 and continuous monitoring phases in the four-phase certification and accreditation process.¹⁰ The primary objective of the security certification phase is to determine if the security controls in the information system are effective in their application (i.e., implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system). The security

⁷ 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.

⁸ 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.

⁹ 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.

¹⁰ FISMA requires the periodic testing and evaluation of the security controls in an information system, to be performed with a frequency depending on risk, but no less than annually. Organizations should maximize the use of assessment results generated during the security certification and continuous monitoring phases of the certification and accreditation process (as defined in NIST Special Publication 800-37) to satisfy the annual FISMA assessment requirements. Reusing security assessment results in this manner promotes a more cost-effective assessment program and reduces unnecessary and duplicative assessment activities.

assessment procedures defined in this publication provide a foundational level of assessment to support the security certification process. As the information system moves into the continuous monitoring phase (subsequent to system authorization during the security accreditation phase), organizations can select an appropriate subset of the assessment methods and procedures defined in this publication to assess the security controls on an ongoing basis. The assessment methods and procedures selected for the follow-on assessments that occur during the continuous monitoring phase (to include annual FISMA assessments) are based on the organization's assessment of risk, the plan of action and milestones for the information system which may indicate the need for greater emphasis on selected security controls, and organizational security policies. The ultimate objective of the continuous monitoring phase is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the hardware, software, and firmware components of the system as well as the environment in which the system operates.

Since some of the security controls required to protect information systems are contained in commercial off-the-shelf (COTS) 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 testing, evaluation, and validation. Product testing, evaluation, and validation are routinely conducted today on cryptographic modules and general-purpose information technology products such as operating systems, database systems, firewalls, intrusion detection devices, web browsers, web applications, smart cards, biometrics devices, personal identity verification devices, web applications, network devices, and hardware platforms using national and international standards such as FIPS 140-2, *Security Requirements for Cryptographic Modules*, and ISO/IEC 15408, *Common Criteria for Information Technology Security Evaluation*. If an information system component product is identified as providing support for the implementation of a particular security control in NIST Special Publication 800-53, then the evidence produced during the product testing, evaluation, and validation processes can be used with other available assessment-related evidence obtained from the application of the assessment methods and procedures in this publication to produce an effective justification and rationale that the security control is effective in its application.¹¹

1.5 REUSE OF ASSESSMENT RESULTS

The reuse of applicable security assessment results from previously accepted/approved assessments of the information system can also be considered in developing the necessary evidence for determining overall security control effectiveness. Applying previous assessment results to a current assessment requires a thorough analysis of the security controls and state of the information system 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 security policies and procedures may be acceptable if it is determined that there have not been any significant changes to the identified policies and procedures. Reusing evidence and security control assessment results produced during the initial certification and accreditation of an information system may be a cost-effective method for supporting continuous monitoring activities and annual FISMA assessments of the information system. Organizations should also consider the amount of time that has transpired since the previous assessments and the degree of independence

¹¹ 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 the information systems where the products are to be deployed.

of the previous assessments. In general, as the time period between current and previous assessments increases, the credibility and utility of the previous assessment results decrease. The degree of independence required from assessment to assessment should also be consistent. For example, it would not be appropriate to reuse results from a previous self-assessment (i.e., lack of assessor independence) in an assessment requiring a higher degree of independence. Finally, organizations should consider the changing conditions associated with security controls over time. Security controls that were deemed effective during previous assessments may have become ineffective due to changing conditions within the information system or the surrounding environment. Thus, assessment results that were found to be previously acceptable may no longer provide credible evidence of security control effectiveness and a reassessment would be required.

1.6 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) the development of effective assurance arguments for security control effectiveness; (ii) the development of effective security assessment plans; (iii) the process of documenting and analyzing assessment results; (iv) the importance of continuous monitoring; and (v) how the assessment results can be used to support the information security programs of organizations.
- **Supporting appendices** provide more detailed security control assessment-related information including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) a description of assessment methods that can be employed by assessors to assess the security controls in organizational information systems; (v) the assessment expectations for low-impact, moderate-impact, and high-impact information systems; (vi) a master catalog of assessment procedures that can be used to develop effective plans for assessing the effectiveness of security controls; (vii) a completed example for effective organization of assessment procedures; and (viii) a summary of minimum assessment procedures for low-impact, moderate-impact, and high-impact information systems.

CHAPTER TWO

THE FUNDAMENTALS

BASIC CONCEPTS ASSOCIATED WITH SECURITY CONTROL ASSESSMENTS

This chapter describes how the assessment procedures contained in this publication were developed including: (i) the conceptual framework used for creating the assessment procedures; (ii) the definitions of individual framework components; (iii) the process employed to generate assessment procedures; and (iv) the organization of the assessment procedures in the master catalog. The information contained in this chapter can be used by organizations to: (i) develop additional assessment procedures that are not contained in the master catalog in Appendix F; or (ii) apply the appropriate level of rigor and intensity to the assessment process for the respective impact levels (low, moderate, or high) of the information system.

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 and to provide guidance for agencies and third parties in developing new or additional assessment procedures, when necessary. 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 NIST Special Publication 800-53 unique identifier for the security control that is the subject of the assessment (e.g., CP-1, CP-4 (1)) and the FIPS 199 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.

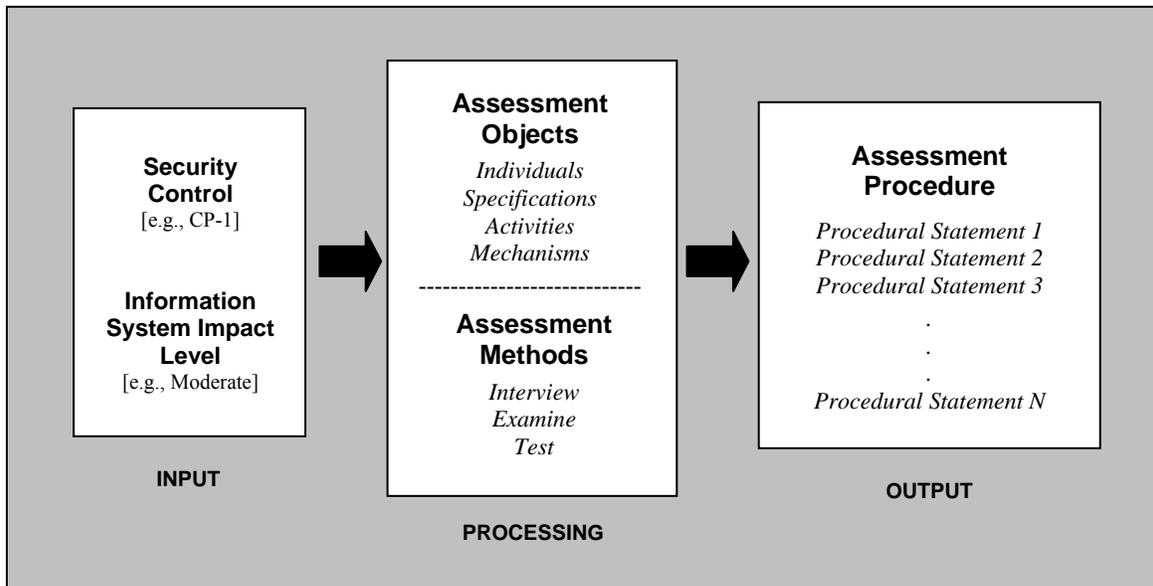


FIGURE 1.1 CONCEPTUAL FRAMEWORK FOR DEVELOPING ASSESSMENT PROCEDURES

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-based 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, or firmware) 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, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities). Similar to the interview method, the primary purpose of the examine method 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 *depth*, *type*, and *coverage*. Attribute definitions and the complete description of each assessment method can be found in Appendix D. Figure 2.1 provides a brief 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)	Generalized	√	---	---
	Focused	---	√	---
	Comprehensive	---	---	√
Type (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.	√	√	√

FIGURE 2.1: ASSESSMENT METHOD ATTRIBUTES AND ATTRIBUTE VALUES BY IMPACT LEVEL

In addition to the assessment method attributes of depth, type, and coverage, 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,¹² 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. The purpose of these activities is to increase the level of confidence that the controls 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.¹³

To help assessors in determining the criteria for security control effectiveness, a set of assessment expectations is provided. The assessment expectations are derived from 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 for a range of assessment objects including specifications, mechanisms, and activities are provided in Appendix E. Figure 2-2 provides a brief summary of the assessment expectations by information systems impact level.

ASSESSMENT EXPECTATIONS	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 2-2: ASSESSMENT EXPECTATIONS BY INFORMATION SYSTEM IMPACT LEVEL

¹² 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.

¹³ For example, the assurance requirements in NIST Special Publication 800-53 at the moderate impact level have been designed to ensure that security controls contain specific actions and the assignment of responsibilities to ensure that the control is implemented or applied within the information system. At the high impact level, the assurance requirements have been designed to ensure that when a security 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 on a continuous basis. These requirements are reflected in the associated security control assessment procedures at the appropriate impact level of the information system being assessed.

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, management commitment, coordination among organizational entities, 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 assessment objects are identified first. 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 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, management commitment, coordination among organizational entities, and compliance, and procedures for implementing contingency planning policy and for each of the associated contingency planning controls.

Having divided the security control into its fundamental parts, the assessment methods are applied to the assessment objects to produce a set of procedural statements that, taken together, comprise the assessment procedure for the security control. The distinct 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 each security control. Thus, the assessment procedure for the security control CP-1, when employed in low-impact information systems and above, consists of the following procedural statements:

CP-1.1. *Examine* organizational records or documents 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, management commitment, coordination among organizational entities, and compliance.

For moderate-impact information systems and above, the following procedural statements are added to the procedural statements used to assess security control CP-1 in low-impact systems:

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.

CP-1.4. Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency planning policy and procedures control is implemented.

For high-impact information systems, the following procedural statements are added to the procedural statements used to assess security control CP-1 in moderate-impact systems:

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. Interview selected organizational personnel with contingency planning and plan implementation responsibilities and **examine** organizational records or documents to determine if the organization consistently applies the contingency planning policy and procedures on an ongoing basis.

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 encountered by the organization in the implementation of the contingency planning policy and procedures control are documented and the resulting information used to actively improve the control 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 defined 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. As stated in the previous section, each assessment procedure consists of multiple procedural statements, which are used in assessing a particular aspect of a security control. Each procedural statement in an assessment procedure contains a unique identifier (e.g., CP-5.2) indicating that this is the second procedural statement for the assessment procedure associated with security control CP-5.

The procedural statements are organized hierarchically in the master catalog by information system impact level. Thus, the procedural statements for assessing security controls in low-impact information systems are presented first. The procedural statements for assessing security controls in moderate-impact information systems are presented next, building upon the statements for low-impact systems. And, finally, the procedural statements for assessing security controls in high-impact information systems are presented last, building on the procedural statements for moderate-impact systems. Similar procedural statements are provided for assessing security control enhancements. The following example in Figure 2.3 illustrates a complete security assessment procedure for the CP-5 security control from the contingency planning family in NIST Special Publication 800-53. The check marks in the table indicate which procedural steps in the assessment procedure apply to the particular security control baseline in Special Publication 800-53 and the FIPS 199 impact level of the information system being assessed.

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-5 CONTINGENCY PLAN UPDATE</p> <p><u>Control:</u> 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.</p>	✓	✓	✓
CP-5.1	<p><i>Examine</i> organizational records or documents to determine if the organization updates the contingency plan in accordance with organization-defined frequency, at least annually.</p>	✓	✓	✓
CP-5.2	<p><i>Examine</i> 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.</p>		✓	✓
CP-5.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan update control is implemented.</p>		✓	✓
CP-5.4	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently reviews and updates the contingency plan on an ongoing basis.</p>			✓
CP-5.5	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency plan update control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FIGURE 2-3: ASSESSMENT PROCEDURE FOR THE CP-5 SECURITY CONTROL

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 methods and procedures from the assessment procedure catalog 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 six steps for developing comprehensive security assessment plans; (iii) the process of documenting and analyzing assessment results; (iv) the importance of continuous monitoring; and (v) how to apply and interpret assessment results to make credible risk-based decisions for information system authorizations to operate.

3.1 BUILDING EFFECTIVE ASSURANCE ARGUMENTS

Today's information systems are incredibly complex assemblages of hardware, software, firmware, and people, 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 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 needed during the assessment process to allow appropriate organizational officials to make credible, risk-based decisions on whether the security controls employed within an information system are effective in their application. The evidence needed to make such assurance arguments is obtained from a variety of sources. The two principal sources of evidence for building effective assurance arguments are obtained from product and system assessments. Product assessments (a.k.a. product evaluations) are typically conducted by independent, third-party testing organizations (e.g., FIPS 140-2 and Common Criteria testing laboratories). Since many information technology products are assessed by commercial testing organizations and then subsequently deployed in millions of information systems worldwide, 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 assessments are typically conducted by information systems developers, systems integrators, certification agents, information system owners, auditors, inspectors general, and the information security staffs of organizations. These assessors or assessment teams bring together the results from product-level assessments, if available, and conduct additional system-level assessments using a variety of methods and techniques. System assessments generate the necessary evidence to determine the overall effectiveness of the security controls employed in the information system and the residual vulnerabilities that may ultimately affect the operations and assets of the organization. The results from assessments conducted using the methods and procedures defined in Special Publication 800-53A provide the minimum acceptable evidence necessary to determine security control effectiveness in accordance with stated assurance requirements.

It is also important to note that the level of detail and extent of assessments can vary greatly depending on the type of assessment and the particular entity conducting the assessment. For example, the most comprehensive assessments are expected to occur during the certification and accreditation process using the full extent of the assessment methods and procedures described in this publication. Other types of assessments (e.g., annual FISMA assessments, self-assessments, audits, and inspections) may provide useful, but far less comprehensive information. In addition to the breadth and depth issues associated with an assessment, organizations should also be cognizant of assessor qualifications (e.g., the technical expertise of the particular assessor or assessment team in the specific hardware, software, and/or firmware components of the information system) when considering the value of the evidence produced to support assurance arguments.¹⁴ Thus, organizations should take into consideration the breadth and depth of the assessments as well as the qualifications of the assessors conducting the assessments when considering the use of such evidence in building assurance arguments for security control effectiveness.

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 documents in the security accreditation package developed by information system owners for authorizing officials.¹⁵ The security assessment report indicates the overall effectiveness of the security controls employed in the 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 may, 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.

There are six distinct steps that assessors should consider in developing a security assessment plan. These steps include: (i) establishing which security controls and control enhancements are to be assessed during the assessment; (ii) selecting the appropriate assessment procedures (and procedural steps) to be used during the assessment of the selected security controls and control enhancements; (iii) developing additional assessment procedures (and procedural statements), if

¹⁴ Phase II of the FISMA Implementation Project addresses the issue of assessor qualifications through the security service provider credentialing program. Additional details on the organizational credentialing program can be obtained from the FISMA Implementation Project web site at <http://csrc.nist.gov/sec-cert>.

¹⁵ 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.

necessary, to address security controls and control enhancements that are not contained in NIST Special Publication 800-53 or to provide additional assurance in security control effectiveness; (iv) optimizing the selected assessment procedures (and procedural steps) to minimize duplication of effort and provide cost-effective assessment solutions; (v) obtaining assessment results from previous assessments and determining the applicability and usefulness of the results; and (vi) finalizing the plan and obtaining the necessary approvals to execute the plan.

Step 1: Establish which security controls are to be included in the assessment.

The security plan for the 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 (i.e., which security controls and control enhancements are to be included in the assessment). Assessors should note which security controls (or parts of controls thereof) 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, or there may be a separate plan to assess the common controls.¹⁶ In either situation, assessors should coordinate the assessment of the security controls in information system with appropriate organizational officials (e.g., chief information officer, senior agency information security officer, authorizing official, information system owner) 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. For each security control in the security plan, assessors should review the corresponding assessment procedure in the catalog of assessment procedures provided in Appendix F. Based on the security category or 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 and an increased level of assurance in the effectiveness of the security controls being assessed. It should be noted that during the tailoring process of the initial security control baseline in accordance with the guidance provided in NIST Special Publication 800-53, selected security controls may have been added, eliminated, or downgraded and/or the organization may have decided to employ compensating controls.¹⁷ The assessment procedures and associated procedural steps should be adjusted accordingly to reflect these changes to the security plan and the security controls in the information system. Organizations should also be aware that certain changes to security controls (i.e., adding and/or deleting controls or control enhancements from the security plan) may affect other controls in the information system and subsequently affect the assessment procedures and procedural steps required to assess the effectiveness of those controls and control enhancements.

¹⁶ NIST Special Publications 800-37 and 800-53 provide guidance on the employment and use of common security controls in organizational information systems.

¹⁷ NIST Special Publication 800-53 provides guidance on the employment and use of compensating controls in organizational information systems.

Step 3: Develop additional assessment procedures and platform/organization specific extensions, if needed.

Based on an assessment of risk, organizations may choose to develop and implement additional security controls or control enhancements 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 and control enhancements. 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 (e.g., access control, identification and authentication, etc.). Detailed test scripts may need to be developed for the specific operating system, network component, middleware, or application employed within the information system to adequately assess certain characteristics of a particular security control. These test scripts are considered extensions of the assessment procedures and procedural statements in Special Publication 800-53A. Platform-specific and organization-specific assessment procedures are beyond the scope of this publication.

Step 4: Optimize the selected assessment procedures to ensure maximum efficiency.

During the assessment of an information system, assessment methods are applied numerous times to a variety of assessment objects within a particular family of security controls. To save time, reduce assessment costs, and maximize the usefulness of assessment results, assessors should review the selected assessment procedures for the security control families and combine or consolidate procedural steps whenever possible or practicable. For example, assessors may wish to consolidate interviews for key organizational officials dealing with a variety of security-related topics. Appendix G provides a detailed example of how assessment procedures may be organized to create an efficient plan to assess the security controls and control enhancements in an organizational information system. Additional efficiencies may be realized by considering potential optimizations across the seventeen security control families in Special Publication 800-53. Assessors have a great deal of flexibility in organizing an assessment plan that meets the needs of the organization and provides the best opportunity to obtaining the necessary evidence to determine security control effectiveness.

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

Assessors should take advantage of assessment results generated during previous security control assessments. Depending on the length of time since the previous assessment, the level of depth/rigor of the assessment process, and the capability and independence¹⁸ of the assessor or assessment team conducting the assessment, assessors may gain significant insights into the state of the security controls in the information system by considering previously generated assessment results. 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 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, and authorizing official) and should not conflict with federal legislation, policies, directives, standards, or guidelines with respect to the assessment of security controls.

¹⁸ NIST Special Publications 800-37 and 800-53 provide guidance on independence in certification agents and certification teams.

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-specific and organization-specific situations, and supplemented with additional information from previous assessments, the assessment plan is finalized and the schedule is established including key milestones for the assessment process. Once the security assessment plan is completed, the plan is reviewed and approved by appropriate organizational officials to ensure that the plan is complete, consistent with the security objectives of the organization and the organization's assessment of risk, and cost-effective with regard to the resources allocated for the assessment.¹⁹

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.²⁰ 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 prescribed by organizational policy, NIST guidance, or OMB policy. The reporting format should be consistent with the type of security control assessment conducted including self-assessments by information system owners, independent verification and validation, independent assessments by certification agents or certification teams supporting a security accreditation process, or independent audits of security controls by auditors. Once the evidence produced by the assessment procedures is 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 been implemented or applied and the vulnerabilities in the information system that may result from this situation.

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 an appropriate body of supporting evidence that all aspects of the security control have been addressed and/or satisfied 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

¹⁹ For self-assessments, the security plan approval step can be omitted.

²⁰ 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.

failure of one or more 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 correcting the noted deficiencies in the security controls. Authorizing officials, in consultation and collaboration with their security staff, 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.²¹ Continuous monitoring, the fourth phase in the security certification and accreditation process, is a proven technique to address the security impacts on information systems resulting from changes to the hardware, software, firmware, or operational environment. 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.²²

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.

Organizations should use the current risk assessment, results of previous security assessments, and operational requirements in guiding the selection of security controls to be monitored and the frequency of the monitoring process. Top priority for control monitoring should be directed at the security controls that have the greatest potential for change after implementation or the controls that have been identified in the organization's plan of action and milestones for the information system. Security control volatility is a measure of how frequently a control is likely

²¹ An effective continuous monitoring program can be used to support the annual FISMA requirement for assessing the security controls in organizational information systems. Organizations should maximize the assessment results produced during the security certification and accreditation process to satisfy annual FISMA assessment requirements.

²² 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.

to change over time after implementation. For example, security policies and implementing procedures in a particular organization may not be likely to change from one year to the next and thus might be considered security controls of low volatility. Access control mechanisms or other technical controls that are subject to the direct effects or side effects of frequent changes in hardware, software, and/or firmware components of an information system may be considered security controls of high volatility. Organizations should apply greater resources to security controls deemed to be of higher volatility as there is a higher return on investment for assessing security controls of this type. Security controls identified in the plan of action and milestones should also be a top priority in the continuous monitoring process due to the fact that these controls have been deemed to be ineffective to some degree (or non-existent, in the worst case). In summary, organizations must make informed judgments regarding the application of limited assessment resources when conducting continuous monitoring activities to ensure that the expenditures are consistent with the organization's mission requirements, security categorization in accordance with FIPS 199, and testing requirements articulated in federal legislation, policy, directives, and regulations.

3.5 APPLYING ASSESSMENT RESULTS

Conducting security assessments in today's complex environment of sophisticated information technology infrastructures and high-visibility, mission-critical applications can be difficult, challenging, and resource-intensive work. However, the stakes have never been higher with regard to ensuring that the security controls employed in federal information systems are effective in their application and provide the essential security needed to protect the operations and assets of federal agencies and the contractors that support those agencies. Success requires the utmost cooperation and collaboration among all parties having a stake in the organization's security well-being, including information system owners, authorizing officials, chief information officers, senior agency information security officers, chief executive officers/heads of agencies, inspectors general, and the OMB. Establishing an appropriate set of expectations before, during, and after the security assessment is paramount to achieving a good outcome—that is, having the capability as an authorizing official, or accreditation authority, to generate the necessary information during the assessment to make a credible, risk-based decision on whether to place the information system into operation or continue its operation. This decision depends largely on the credibility of the information produced during the security assessment which contributes to understanding the residual vulnerabilities in the information system after the application of an agreed-upon set of security controls and the ultimate acceptance of risk to the organization's mission.

Security assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits—rather, they are the last line of defense in knowing the strengths and weaknesses of an organization's information system which is supporting critical federal applications and missions in a global environment of sophisticated threats. Security assessment results are used primarily to determine the overall effectiveness of the security controls in an information system, identify residual vulnerabilities in the system, and provide credible and meaningful inputs to the organization's Plan of Action and Milestones (POA&M). A well-executed security assessment validates the security controls contained in the information system security plan and facilitates a cost-effective approach to correcting deficiencies in the system in an orderly and disciplined manner consistent with the organization's mission requirements.

APPENDIX A

REFERENCES

LAWS, DIRECTIVES, POLICIES, STANDARDS, AND GUIDELINES²³

LEGISLATION
1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
DIRECTIVES, POLICIES, AND INSTRUCTIONS
3. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, <i>Management of Federal Information Resources</i> , November 2000.
4. Office of Management and Budget Memorandum M-02-01, <i>Guidance for Preparing and Submitting Security Plans of Action and Milestones</i> , October 2001.
5. Office of Management and Budget Memorandum M-03-22, <i>OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002</i> , September 2003.
STANDARDS
6. National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, <i>Security Requirements for Cryptographic Modules</i> , May 2001.
7. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i> , February 2004.
8. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, <i>Minimum Security Requirements for Federal Information and Information Systems</i> , March 2006.
9. National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, <i>Personal Identity Verification (PIV) of Federal Employees and Contractors</i> , March 2006.
10. Committee for National Security Systems (CNSS) Instruction 4009, <i>National Information Assurance Glossary</i> , May 2003.
11. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, <i>Protective Distribution Systems (PDS)</i> , December 1996.
GUIDELINES
12. National Institute of Standards and Technology Special Publication 800-12, <i>An Introduction to Computer Security: The NIST Handbook</i> , October 1995.
13. National Institute of Standards and Technology Special Publication 800-16, <i>Information Technology Security Training Requirements: A Role- and Performance-Based Model</i> , April 1998.

²³ The status and most current versions of NIST publications including FIPS and Special Publications in the 800-series (draft and final) can be found at <http://csrc.nist.gov/publications>.

14. National Institute of Standards and Technology Special Publication 800-18, Revision 1, <i>Guide for Developing Security Plans for Federal Information Systems</i> , February 2006.
15. National Institute of Standards and Technology Special Publication 800-23, <i>Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products</i> , August 2000.
16. National Institute of Standards and Technology Special Publication 800-26, <i>Security Self-Assessment Guide for Information Technology Systems</i> , November 2001.
17. National Institute of Standards and Technology Special Publication 800-27, <i>Engineering Principles for Information Technology Security (A Baseline for Achieving Security)</i> , Revision A, June 2004.
18. National Institute of Standards and Technology Special Publication 800-28, <i>Guidelines on Active Content and Mobile Code</i> , October 2001.
19. National Institute of Standards and Technology Special Publication 800-30, <i>Risk Management Guide for Information Technology Systems</i> , July 2002.
20. National Institute of Standards and Technology Special Publication 800-32, <i>Introduction to Public Key Technology and the Federal PKI Infrastructure</i> , February 2001.
21. National Institute of Standards and Technology Special Publication 800-34, <i>Contingency Planning Guide for Information Technology Systems</i> , June 2002.
22. National Institute of Standards and Technology Special Publication 800-35, <i>Guide to Information Technology Security Services</i> , October 2003.
23. National Institute of Standards and Technology Special Publication 800-36, <i>Guide to Selecting Information Security Products</i> , October 2003.
24. National Institute of Standards and Technology Special Publication 800-37, <i>Guide for the Security Certification and Accreditation of Federal Information Systems</i> , May 2004.
25. National Institute of Standards and Technology Special Publication 800-40, Version 2.0, <i>Creating a Patch and Vulnerability Management Program</i> , November 2005.
26. National Institute of Standards and Technology Special Publication 800-42, <i>Guideline on Network Security Testing</i> , October 2003.
27. National Institute of Standards and Technology Special Publication 800-45, <i>Guidelines on Electronic Mail Security</i> , September 2002.
28. National Institute of Standards and Technology Special Publication 800-46, <i>Security for Telecommuting and Broadband Communications</i> , August 2002.
29. National Institute of Standards and Technology Special Publication 800-47, <i>Security Guide for Interconnecting Information Technology Systems</i> , August 2002.
30. National Institute of Standards and Technology Special Publication 800-48, <i>Wireless Network Security: 802.11, Bluetooth, and Handheld Devices</i> , November 2002.
31. National Institute of Standards and Technology Special Publication 800-50, <i>Building an Information Technology Security Awareness and Training Program</i> , October 2003.
32. National Institute of Standards and Technology Special Publication 800-52, <i>Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations</i> , June 2005.

33. National Institute of Standards and Technology Special Publication 800-53, Revision 1, <i>Recommended Security Controls for Federal Information Systems</i> , (Draft) March 2006.
34. National Institute of Standards and Technology Special Publication 800-56A, <i>Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography</i> , March 2006.
35. National Institute of Standards and Technology Special Publication 800-57, <i>Recommendation on Key Management, Parts 1 and 2</i> , August 2005.
36. National Institute of Standards and Technology Special Publication 800-58, <i>Security Considerations for Voice Over IP Systems</i> , January 2005.
37. National Institute of Standards and Technology Special Publication 800-59, <i>Guideline for Identifying an Information System as a National Security System</i> , August 2003.
38. National Institute of Standards and Technology Special Publication 800-60, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i> , June 2004.
39. National Institute of Standards and Technology Special Publication 800-61, <i>Computer Security Incident Handling Guide</i> , January 2004.
40. National Institute of Standards and Technology Special Publication 800-63, Version 1.0.1, <i>Electronic Authentication Guideline</i> , September 2004.
41. National Institute of Standards and Technology Special Publication 800-64, Revision 1, <i>Security Considerations in the Information System Development Life Cycle</i> , June 2004.
42. National Institute of Standards and Technology Special Publication 800-65, <i>Integrating Security into the Capital Planning and Investment Control Process</i> , January 2005.
43. National Institute of Standards and Technology Special Publication 800-70, <i>Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers</i> , May 2005.
44. National Institute of Standards and Technology Special Publication 800-73, Revision 1, <i>Interfaces for Personal Identity Verification</i> , March 2006.
45. National Institute of Standards and Technology Special Publication 800-76, <i>Biometric Data Specification for Personal Identity Verification</i> , February 2006.
46. National Institute of Standards and Technology Special Publication 800-77, <i>Guide to IPsec VPNs</i> , December 2005.
47. National Institute of Standards and Technology Special Publication 800-78, <i>Cryptographic Algorithms and Key Sizes for Personal Identity Verification</i> , April 2005.
48. National Institute of Standards and Technology Special Publication 800-79, <i>Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations</i> , July 2005.
49. National Institute of Standards and Technology Special Publication 800-81, <i>Secure Domain Name System (DNS) Deployment Guide</i> (Draft), August 2005.
50. National Institute of Standards and Technology Special Publication 800-83, <i>Guide to Malware Incident Prevention and Handling</i> , November 2005.
51. National Institute of Standards and Technology Special Publication 800-85A, <i>PIV Middleware and PIV Card Application Conformance Test Guidelines</i> , April 2006.

52. National Institute of Standards and Technology Special Publication 800-88, <i>Guidelines for Media Sanitization</i> (Draft), February 2006.
53. National Institute of Standards and Technology Special Publication 800-95, <i>Risk Assessments and the System Security Life Cycle: A Coordinated Approach</i> (Draft), April 2006.
MISCELLANEOUS PUBLICATIONS
54. Department of Health and Human Services Centers for Medicare and Medicaid Services (CMS), <i>Core Set of Security Requirements</i> , February 2004.
55. Government Accountability Office <i>Federal Information System Controls Audit Manual</i> , GAO/AIMD-12.19.6, January 1999.

Draft

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*.

TERM	DEFINITION
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.

TERM	DEFINITION
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 [NIST SP 800-53]	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.

TERM	DEFINITION
Configuration Control [CNSS Inst. 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to ensure that 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 governmentwide 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.
Functional Testing	A test methodology that assumes knowledge of the functional specifications, high-level design, and operating specifications of the item under assessment. Also known as black box testing.
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 [NIST SP 800-53]	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.

TERM	DEFINITION
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 [NIST SP 800-53]	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.

TERM	DEFINITION
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, or firmware) 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.
Media Sanitization [NIST SP 800-88]	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
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 [NIST SP 800-53]	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.

TERM	DEFINITION
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).
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
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.

TERM	DEFINITION
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a <i>limited</i> adverse effect (FIPS 199 low); (ii) a <i>serious</i> adverse effect (FIPS 199 moderate); or (iii) a <i>severe</i> or <i>catastrophic</i> 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 that 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.

TERM	DEFINITION
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.
Scoping Guidance [NIST SP 800-53]	Provides organizations with specific policy/regulatory-related, 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 Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an 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.
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 [NIST SP 800-53]	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
Security Control Enhancements [NIST SP 800-53]	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.

TERM	DEFINITION
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 [NIST SP 800-53]	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-based 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.
Structural Testing	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). Also known as "gray-box" or "white-box" testing.
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.

TERM	DEFINITION
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
U.S.C.	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

ASSESSMENT OBJECTS: Individuals or groups of individuals.

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

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include interviewing agency heads, chief information officers, senior agency information security officers, authorizing officials, 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) generalized; (ii) focused; and (iii) comprehensive.
 - *Generalized* interviews: Interviews that consist of broad, high-level discussions with selected organizational personnel on particular topics relating to the security controls being assessed. This type of interview is typically conducted using a set of generalized, high-level questions and is intended to capture a broad, general understanding of the fundamental concepts associated with specifications, mechanisms, or activities.
 - *Focused* interviews: Interviews that consist of broad, high-level discussions **and more detailed discussions in specific areas** with selected organizational personnel on particular topics relating to the security controls being assessed. 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 responses indicate a need for more detailed investigation** and is intended to capture the **specific** understanding of the fundamental concepts associated with specifications, mechanisms, or activities.
 - *Comprehensive* interviews: Interviews that consist of broad, high-level discussions and more detailed, **probing** discussions in specific areas with selected organizational personnel on particular topics relating to the security controls 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, **probing** questions in specific areas where responses indicate a need for more detailed investigation **or where assessment evidence allows** and is intended to capture the specific understanding of the fundamental concepts **and implementation details** associated with specifications, mechanisms, or activities.
- The *coverage* attribute addresses the categories of individuals to be interviewed (by organizational roles and associated responsibilities) and the number of individuals to be interviewed (by category). Organizations, in collaboration with information system assessors, determine the specific categories and numbers of individuals to be interviewed during the assessment process.

ASSESSMENT METHOD: Examine

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

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.

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 categories 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) generalized; (ii) focused; and (iii) comprehensive.
 - *Generalized* examinations: Examinations that consist of brief, high-level reviews, observations, or inspections of security controls using a limited body of evidence or documentation. These types of examinations are typically conducted using functional-level descriptions of specifications, mechanisms, or activities.
 - *Focused* examinations: Examinations that consist of **detailed analyses** of security controls using a **substantial** body of evidence or documentation. These types of examinations are typically conducted using functional-level descriptions of specifications, mechanisms, or activities, **and where appropriate, high-level design information**.
 - *Comprehensive* examinations: Examinations that consist of detailed **and thorough** analyses of security controls using **an extensive** body of evidence or documentation. 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).
- The *coverage* attribute addresses the categories of specifications, mechanisms, or activities to be examined and the number of specifications, mechanisms, or activities to be examined (by category). Organizations, in collaboration with information system assessors, determine the specific categories and numbers of specifications, mechanisms, or activities to be assessed during the assessment process.

ASSESSMENT METHOD: Test

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

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.²⁴

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.²⁵ Applying the test method to a particular security control may require testing multiple assessment objects of different categories. The number and categories 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: Type, Coverage

- The *type* attribute addresses the types of testing to be conducted. There are three possible values for the type attribute: (i) functional testing; (ii) penetration testing; and (iii) structural testing.
 - *Functional* testing: A test methodology that assumes knowledge of the functional specifications, high-level design, and operating specifications of the item under assessment. Also known as “black box” testing.
 - *Penetration* testing: A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
 - *Structural* testing: 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). Also known as “gray box” or “white box” testing.
- The *coverage* attribute addresses the categories of mechanisms or activities to be tested and the number of mechanisms or activities to be tested (by category). Organizations, in collaboration with information system assessors, determine the specific categories 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.).

²⁴ 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.

²⁵ 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)	Generalized	√	---	---
	Focused	---	√	---
	Comprehensive	---	---	√
Type (Test method only)	Functional (black-box)	√	√	√
	Penetration	---	√	√
	Structural (gray-box, white-box)	---	---	√
Coverage (All methods)	Categories and number of assessment objects determined by organizations in collaboration with assessors. ²⁶	√	√	√

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

²⁶ The categories and number 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 categories and number of objects assessed as the impact level of the information system increases. The increased coverage and depth of the assessment as well as the type of testing employed during the 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. The use of bolded text in the assurance requirements and assessment expectations indicates additions to the requirements or expectations that appear for the first time at a particular information system impact level.

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, 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: Generalized 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.
- The assessor determines if the specification, as written, is consistent with the functional requirements in the security control statement.

For *mechanisms*:

- The assessor determines if the mechanism is implemented and operational.
- The assessor determines if the mechanism, as implemented, is consistent with the functional requirements in the security control statement.

For *activities*:

- The assessor determines if the activity is being performed.
- The assessor determines if the activity, as performed, 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. This documentation is also needed by assessors to analyze and test the functional properties of the control as part of the overall assessment of the control.

Assessment Expectations: Focused 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.
- The assessor determines if the specification, as written, is consistent with the functional requirements in the security control statement.
- **The assessor determines if the organization provides an assignment of responsibilities and specific actions to ensure that the specification is being applied/followed and meets its required function or purpose.**

For *mechanisms*:

- The assessor determines if the mechanism is implemented and operational.
- The assessor determines if the mechanism, as implemented, is consistent with the functional requirements in the security control statement.
- **The assessor determines if the organization provides an assignment of responsibilities and specific actions to ensure that the mechanism is being employed and meets its required function or purpose.**

For *activities*:

- The assessor determines if the activity is being performed.
- The assessor determines if the activity, as performed, is consistent with the functional requirements in the security control statement.
- **The assessor determines if the organization provides an assignment of responsibilities and specific actions to ensure that 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. This documentation is also 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.
- The assessor determines if the specification, as written, is consistent with the functional requirements in the security control statement.
- The assessor determines if the organization provides an assignment of responsibilities and specific actions to ensure that the specification is being applied/followed and meets its required function or purpose **consistently on an ongoing basis**.
- **The assessor determines if the organization provides a means to support the continuous improvement in the effectiveness of the specification, as appropriate.**

For *mechanisms*:

- The assessor determines if the mechanism is implemented and operational.
- The assessor determines if the mechanism, as implemented, is consistent with the functional requirements in the security control statement.
- The assessor determines if the organization provides an assignment of responsibilities and specific actions to ensure that the mechanism is being employed and meets its required function or purpose **consistently on an ongoing basis**.
- **The assessor determines if the organization provides a means to support the continuous improvement in the effectiveness of the mechanism, as appropriate.**

For *activities*:

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

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

ASSESSMENT EXPECTATIONS	INFORMATION SYSTEM IMPACT LEVEL		
	LOW	MODERATE	HIGH
Security controls in place; no obvious errors.	√	√	√
Security controls appropriately formulated/unambiguous; or Security controls correctly implemented/operating as intended.	---	√	√
Security controls consistently applied on an ongoing basis with continuous improvement.	---	---	√

FIGURE E-1: ASSESSMENT EXPECTATIONS BY INFORMATION SYSTEM IMPACT LEVEL

APPENDIX F

ASSESSMENT PROCEDURE CATALOG

METHODS, OBJECTS, AND PROCEDURES FOR ASSESSING SECURITY CONTROLS

This appendix provides a catalog of assessment procedures for the security controls in NIST Special Publication 800-53. The assessment procedures are organized by families similar to the security control catalog in Special Publication 800-53. Each procedure consists of multiple procedural statements, which are used in assessing some particular aspect of a security control. Each procedural statement in the assessment procedure contains a unique identifier (e.g., CP-3.2) indicating that this is the second procedural statement used to assess the effectiveness of security control CP-3. The procedural statements are organized hierarchically by information system impact level. Thus, the procedural statements for assessing security controls in low-impact information systems are presented first. The procedural statements for assessing security controls in moderate-impact information systems are presented next, building upon the previous statements for low-impact systems. And, finally, the procedural statements for assessing security controls in high-impact information systems are presented last, building on the previous statements for low- and moderate-impact systems. Procedural statements for assessing security control enhancements follow the same format but are only applied to moderate- and high-impact information systems (following the convention established in Special Publication 800-53). There are procedural statements in the master catalog that might not be used by assessors because the associated security control or control enhancement does not appear in any security control baseline (i.e., it is not a minimum security control or control enhancement in the low, moderate, or high baseline in Special Publication 800-53). These additional procedural statements are available to assessors, however, in situations where the additional security controls or control enhancements are selected and employed within the information system and require assessment.

Each procedural statement identifies the assessment method or methods to be used in the assessment of the security control, but does not reflect the extent, rigor, and level of intensity of the assessment process as defined by the attributes (e.g., depth, coverage, or type) 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 assessment method attributes.

In preparation for the assessment of security controls, a significant amount of background information should be assembled and made available to the assessors or assessment team. The organization should identify and arrange access to: (i) elements of the organization responsible for developing, documenting, disseminating, reviewing, and updating all security policies and associated procedures for implementing the policies; (ii) the security policies for the information system and any associated implementing procedures; (iii) individuals or groups responsible for the development, implementation, operation, and maintenance of security procedures; (iv) any materials (e.g., security plans, records, schedules, assessment reports, after-action reports, agreements, accreditation packages) associated with the implementation of security procedures and operations; and (v) the number/percentage of objects to be assessed by category. The preparation and availability of essential documentation as well as access to key organizational personnel are paramount to a successful assessment of the information system security controls.

ASSESSMENT PROCEDURES

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-1 ACCESS CONTROL POLICY AND PROCEDURES</p> <p><u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.</p>	✓	✓	✓
AC-1.1	<p><i>Examine</i> organizational records or documents 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.</p>	✓	✓	✓
AC-1.2	<p><i>Examine</i> the access control policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</p>	✓	✓	✓
AC-1.3	<p><i>Examine</i> 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.</p>		✓	✓
AC-1.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control policy and procedures control is implemented.</p>		✓	✓
AC-1.5	<p><i>Examine</i> 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.</p>			✓
AC-1.6	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies the access control policy and procedures on an ongoing basis.</p>			✓
AC-1.7	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access control policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-2 ACCOUNT MANAGEMENT</p> <p><u>Control:</u> 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].</p>	✓	✓	✓
AC-2.1	<i>Examine</i> organizational records or documents to determine if the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.	✓	✓	✓
AC-2.2	<i>Examine</i> organizational records or documents to determine if the organization conducts information system account reviews within the prescribed organization-defined frequency and any required actions as a result of the reviews have occurred in accordance with established procedures.	✓	✓	✓
AC-2.3	<i>Examine</i> selected active user accounts to determine if the organization followed procedures to establish and activate the user accounts and completed any organization-required documentation.		✓	✓
AC-2.4	<i>Examine</i> a list of recently disabled information system accounts and compare to selected system-generated records with user IDs and last login date for each account to determine if the last log-in date is beyond the date that the account is disabled.		✓	✓
AC-2.5	<i>Examine</i> a list of recently separated or terminated employees to determine if the organization removed accounts for these individuals according to established procedures and completed any organization-required documentation.		✓	✓
AC-2.6	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the account management control is implemented.		✓	✓
AC-2.7	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently manages information system accounts on an ongoing basis.			✓
AC-2.8	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the account management control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AC-2 ACCOUNT MANAGEMENT Control Enhancement: (1) The organization employs automated mechanisms to support the management of information system accounts.		✓	✓
AC-2.9	<i>Examine organizational records or documents to determine if the organization employs automated mechanisms to support information system account management functions and how those mechanisms are implemented.</i>		✓	✓
AC-2.10	<i>Test selected automated mechanisms within the information system that support the account management functions to determine if the mechanisms are operating as intended and the account management activities are properly conducted.</i>			✓
	AC-2 ACCOUNT MANAGEMENT Control Enhancement: (2) The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].		✓	✓
AC-2.11	<i>Examine organizational records or documents to determine if temporary and emergency accounts are automatically terminated after [organization-defined time period] for each type of account.</i>		✓	✓
AC-2.12	<i>Examine the information system configuration settings to determine if the settings are set to automatically terminate temporary and emergency accounts after [organization-defined time period].</i>		✓	✓
AC-2.13	<i>Examine organizational records or documents to determine if any temporary or emergency accounts have not been terminated after [organization-defined time period].</i>			✓
AC-2.14	<i>Test the information system to determine if temporary and emergency accounts are automatically terminated after exceeding a set time period.</i>			✓
	AC-2 ACCOUNT MANAGEMENT Control Enhancement: (3) The information system automatically disables inactive accounts after [Assignment: organization-defined time period].		✓	✓
AC-2.15	<i>Examine organizational records or documents to determine if inactive accounts on the information system are automatically disabled after [organization-defined time period].</i>		✓	✓
AC-2.16	<i>Examine the information system configuration settings to determine if the settings are set to automatically disable inactive accounts after [organization-defined time period].</i>		✓	✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
AC-2.17	<i>Examine</i> organizational records or documents to determine if any inactive accounts on the information system have not been disabled after [organization-defined time period], (i.e., if the last login date exceeds the organization-defined time period for disabling inactive accounts).			✓
AC-2.18	<i>Test</i> the information system to determine if inactive accounts are automatically disabled after exceeding [organization-defined time period].			✓
	AC-2 ACCOUNT MANAGEMENT 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-2.19	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and that appropriate individuals are notified of these occurrences.			✓
AC-2.20	<i>Test</i> selected automated mechanisms within the information system that support the account management auditing and notification functions to determine if: (i) the mechanisms are operating as intended; (ii) each of the account actions identified produce accurate and informative audit records; and (iii) each action, as required by the account management procedures, results in notification of appropriate individuals.			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AC-3 ACCESS ENFORCEMENT <u>Control:</u> The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	✓	✓	✓
AC-3.1	<i>Examine</i> organizational records or documents to determine if user access to the information system is authorized.	✓	✓	✓
AC-3.2	<i>Examine</i> access control mechanisms to determine if the information system is configured to implement the organizational access control policy.	✓	✓	✓
AC-3.3	<i>Examine</i> the user access rights on the information system to determine if user privileges on the system are consistent with the documented user authorizations.		✓	✓
AC-3.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access enforcement control is implemented.		✓	✓
AC-3.5	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently enforces assigned authorizations for controlling access to the system on an ongoing basis.			✓
AC-3.6	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access enforcement control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	AC-3 ACCESS ENFORCEMENT <u>Control Enhancement:</u> (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	<i>Examine</i> organizational records or documents to determine if the organization explicitly defines security functions for the information system.		✓	✓
AC-3.8	<i>Examine</i> organizational records or documents to determine if the organization properly authorizes personnel granted access to security functions and information in accordance with organizational policy.		✓	✓
AC-3.9	<i>Test</i> 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.			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-4 INFORMATION FLOW ENFORCEMENT</p> <p><u>Control:</u> The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.</p>		✓	✓
AC-4.1	<p><i>Examine</i> 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.</p>		✓	✓
AC-4.2	<p><i>Examine</i> 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.</p>		✓	✓
AC-4.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information flow enforcement control is implemented.</p>		✓	✓
AC-4.4	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems on an ongoing basis.</p>			✓
AC-4.5	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information flow enforcement control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-5 SEPARATION OF DUTIES <u>Control:</u> The information system enforces separation of duties through assigned access authorizations.</p>		✓	✓
AC-5.1	<p><i>Examine</i> organizational records or documents to determine if the information system enforces separation of duties.</p>		✓	✓
AC-5.2	<p><i>Examine</i> organizational records or documents 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.</p>		✓	✓
AC-5.3	<p><i>Examine</i> selected information system accounts to determine if any user has access authorizations or privileges that may allow the user to perform multiple conflicting 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).</p>		✓	✓
AC-5.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the separation of duties control is implemented.</p>		✓	✓
AC-5.5	<p><i>Test</i> access control mechanisms by attempting to assign an individual user multiple, conflicting roles within the information system to determine if the system allows a single user to perform multiple functions/roles in violation of the separation of duties policy.</p>			✓
AC-5.6	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently enforces assigned authorizations to support separation of duties on an ongoing basis.</p>			✓
AC-5.7	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the separation of duties control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-6 LEAST PRIVILEGE</p> <p><u>Control:</u> 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.</p>		✓	✓
AC-6.1	<i>Examine</i> organizational records or documents to determine if the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.		✓	✓
AC-6.2	<i>Examine</i> organizational records or documents to determine what access rights/privileges the organization assigns to user tasks.		✓	✓
AC-6.3	<i>Examine</i> 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.		✓	✓
AC-6.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least privilege control is implemented.		✓	✓
AC-6.5	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently enforces the most restrictive set of rights/privileges or accesses needed by users on an ongoing basis.			✓
AC-6.6	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the least privilege control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-7 UNSUCCESSFUL LOGIN ATTEMPTS</p> <p><u>Control:</u> 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.</p>	✓	✓	✓
AC-7.1	<p>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.</p>	✓	✓	✓
AC-7.2	<p>Examine the information system configuration settings to determine if the information system enforces organizational policy and procedures for unsuccessful login attempts.</p>	✓	✓	✓
AC-7.3	<p>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.</p>		✓	✓
AC-7.4	<p>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the unsuccessful login attempts control is implemented.</p>		✓	✓
AC-7.5	<p>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.</p>			✓
AC-7.6	<p>Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently enforces limitations on consecutive invalid access attempts on an ongoing basis.</p>			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
AC-7.7	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the unsuccessful login attempts control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	<p>AC-7 UNSUCCESSFUL LOGIN ATTEMPTS <u>Control Enhancement:</u> (1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.</p>			
AC-7.8	<i>Examine</i> 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.			
AC-7.9	<i>Test</i> 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.			

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-8 SYSTEM USE NOTIFICATION</p> <p><u>Control:</u> 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.</p>	✓	✓	✓
AC-8.1	<p><i>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).</i></p>	✓	✓	✓
AC-8.2	<p><i>Interview organizational personnel with access control responsibilities and examine organizational records or documents for approval of the information system use notification message before its use.</i></p>		✓	✓
AC-8.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system use notification control is implemented.</i></p>		✓	✓
AC-8.4	<p><i>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.</i></p>			✓
AC-8.5	<p><i>Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the information system consistently displays the system use notification message on an ongoing basis.</i></p>			✓
AC-8.6	<p><i>Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system use notification control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-9 PREVIOUS LOGON NOTIFICATION <u>Control:</u> 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.</p>			
AC-9.1	<p><i>Examine</i> 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.</p>			
AC-9.2	<p><i>Test</i> the information system by viewing a selection of user logons 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.</p>			
AC-9.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the previous logon notification control is implemented.</p>			
AC-9.4	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently provides users with essential logon information on an ongoing basis.</p>			
AC-9.5	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the previous logon notification control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AC-10 CONCURRENT SESSION CONTROL <u>Control:</u> The information system limits the number of concurrent sessions for any user to [Assignment: organization-defined number of sessions].			✓
AC-10.1	<i>Examine</i> 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.			✓
AC-10.2	<i>Test</i> the concurrent session control by attempting to exceed the organization-defined number of concurrent sessions with a valid user account.			✓
AC-10.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the concurrent session control is implemented.			✓
AC-10.4	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently limits the number of concurrent sessions on an ongoing basis.			✓
AC-10.5	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the concurrent session control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-11 SESSION LOCK</p> <p><u>Control:</u> 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.</p>		✓	✓
AC-11.1	<i>Examine</i> 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.		✓	✓
AC-11.2	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the session lock control is implemented.		✓	✓
AC-11.3	<i>Test</i> 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 the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.			✓
AC-11.4	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently employs a session lock capability on an ongoing basis.			✓
AC-11.5	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the session lock control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-12 SESSION TERMINATION <u>Control:</u> The information system automatically terminates a session after [Assignment: organization-defined time period] of inactivity.</p>		✓	✓
AC-12.1	<p><i>Examine</i> the configuration settings of the information system to determine if the system automatically terminates a session after [organization-defined time period] of inactivity.</p>		✓	✓
AC-12.2	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the session termination control is implemented.</p>		✓	✓
AC-12.3	<p><i>Test</i> the session termination mechanism by allowing a valid user session to remain inactive for [organization-defined time period] to determine if the session automatically terminates.</p>			✓
AC-12.4	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently employs a session termination capability on an ongoing basis.</p>			✓
AC-12.5	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the session termination control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL <u>Control:</u> The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.	✓	✓	✓
AC-13.1	<i>Interview selected organizational personnel with access control responsibilities to determine if the organization supervises and reviews the activities of users of the information system.</i>	✓	✓	✓
AC-13.2	<i>Examine organizational records or documents to determine if unusual activity is investigated, reported to appropriate officials, and resolved.</i>	✓	✓	✓
AC-13.3	<i>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.</i>		✓	✓
AC-13.4	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the supervision and review of access control is implemented.</i>		✓	✓
AC-13.5	<i>Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently supervises and reviews user activities with respect to the enforcement and use of access controls for the information system on an ongoing basis.</i>			✓
AC-13.6	<i>Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the supervision and review of access control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓
	AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL <u>Control Enhancement:</u> (1) The organization employs automated mechanisms to facilitate the review of user activities.			✓
AC-13.7	<i>Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities and how those mechanisms are implemented.</i>			✓
AC-13.8	<i>Examine the configuration of the automated mechanism(s) within the information system to determine if the mechanisms support the review of user activities.</i>			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
AC-13.9	<i>Examine the output from the automated mechanism(s) within the information system to determine if each of the automated functions associated with the review of user activities produces accurate and informative information to support and facilitate the review of user activities with respect to access control enforcement and usage.</i>			✓

Draft

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION</p> <p><u>Control:</u> The organization identifies specific user actions that can be performed on the information system without identification or authentication.</p>	✓	✓	✓
AC-14.1	<i>Examine</i> organizational records or documents to determine what specific user actions can be performed on the information system without requiring identification and authentication.	✓	✓	✓
AC-14.2	<i>Examine</i> 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.	✓	✓	✓
AC-14.3	<i>Test</i> 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.		✓	✓
AC-14.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the permitted actions without identification and authentication control is implemented.		✓	✓
AC-14.5	<i>Test</i> the information system by attempting to perform actions that are not permitted for a user that has not been identified or authenticated to the information system (e.g., administrator functions).			✓
AC-14.6	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently identifies actions permitted on the information system without requiring user identification or authentication on an ongoing basis.			✓
AC-14.7	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the permitted actions without identification and authentication control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION <u>Control Enhancement:</u> (1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.</p>		✓	✓
AC-14.8	<p><i>Examine organizational records or documents to determine if the organization limits specific user actions that can be performed without identification and authentication to only the actions required to accomplish mission objectives.</i></p>		✓	✓
AC-14.9	<p><i>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.</i></p>		✓	✓
AC-14.10	<p><i>Test the information system by attempting to perform actions that are not defined by the access control policy and procedures as being the minimum actions necessary to accomplish mission objectives without identification and authentication, to determine if the access controls are working as intended.</i></p>			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-15 AUTOMATED MARKING</p> <p><u>Control:</u> The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.</p>			✓
AC-15.1	<i>Examine</i> information system output to determine if standard naming conventions are used to identify any special dissemination, handling, or distribution instructions.			✓
AC-15.2	<i>Examine</i> the configuration of the information system to determine how the system automatically marks the output for any special disseminating, handling or distribution instructions.			✓
AC-15.3	<i>Test</i> the automated marking capability in the information system 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 the automated marking policy and procedures.			✓
AC-15.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the automated marking control is implemented.			✓
AC-15.5	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently implements automated marking of information system output on an ongoing basis.			✓
AC-15.6	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the automated marking control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-16 AUTOMATED LABELING <u>Control:</u> The information system appropriately labels information in storage, in process, and in transmission.</p>			
AC-16.1	<p><i>Examine</i> selected information contained within the information system to determine if labels are accurately in place and in accordance with organizational policy and procedures.</p>			
AC-16.2	<p><i>Examine</i> the configuration settings of the information system to determine if the system labels information in storage, in process, and in transmission.</p>			
AC-16.3	<p><i>Test</i> 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.</p>			
AC-16.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the automated labeling control is implemented.</p>			
AC-16.5	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently employs an automated labeling capability on an ongoing basis.</p>			
AC-16.6	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the automated labeling control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-17 REMOTE ACCESS</p> <p><u>Control:</u> 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.</p>	✓	✓	✓
AC-17.1	<p><i>Examine</i> organizational records or documents to determine if remote access is: (i) monitored on a periodic basis in accordance with organization policy; (ii) restricted through dial-up connections or protects against unauthorized connections or subversion of unauthorized connections; (iii) authorized and restricted to users with an operational need for access; and (iv) restricted to only allow privileged access based on compelling operational needs.</p>	✓	✓	✓
AC-17.2	<p><i>Examine</i> 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.</p>		✓	✓
AC-17.3	<p><i>Examine</i> organizational records or documents to determine if remote access is documented and authorized by the appropriate organization officials.</p>		✓	✓
AC-17.4	<p><i>Examine</i> the configuration of the information system to determine if controls are employed to restrict remote access to the system.</p>		✓	✓
AC-17.5	<p><i>Examine</i> 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.</p>		✓	✓
AC-17.6	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote access control is implemented.</p>		✓	✓
AC-17.7	<p><i>Test</i> 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.</p>		✓	✓
AC-17.8	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently employs remote access controls for the information system on an ongoing basis.</p>			✓
AC-17.9	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the remote access control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AC-17 REMOTE ACCESS <u>Control Enhancement:</u> (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.		✓	✓
AC-17.10	<i>Examine</i> organizational records or documents to determine what automated mechanisms and functions are employed to support and facilitate the monitoring and control of remote access methods.		✓	✓
AC-17.11	<i>Examine</i> organizational records or documents to determine if the automated mechanisms supporting the monitoring and control of remote access are effectively employed in accordance with organizational policy and procedures.		✓	✓
AC-17.12	<i>Test</i> the automated mechanism(s) within the information system to determine if each of the functions associated with the monitoring and control of remote access produce accurate and informative information, in accordance with remote access monitoring policy and procedures.			✓
	AC-17 REMOTE ACCESS <u>Control Enhancement:</u> (2) The organization uses encryption to protect the confidentiality of remote access sessions.		✓	✓
AC-17.13	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> the configuration of the information system to determine if the organization uses encryption to protect the confidentiality of remote access sessions.		✓	✓
AC-17.14	<i>Examine</i> a remote access connection to the information system to determine if the connection requires the use of encryption and encryption is actually employed.			✓
	AC-17 REMOTE ACCESS <u>Control Enhancement:</u> (3) The organization controls all remote accesses through a managed access control point.		✓	✓
AC-17.15	<i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> the configuration of the information system to determine if the organization controls remote access through a managed access control point.		✓	✓
AC-17.16	<i>Test</i> 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 organizational policy and procedures.			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-18 WIRELESS ACCESS RESTRICTIONS</p> <p><u>Control:</u> 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.</p>	✓	✓	✓
AC-18.1	<p><i>Examine</i> organizational records or documents 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.</p>	✓	✓	✓
AC-18.2	<p><i>Examine</i> organizational records or documents to determine if the access control policy and procedures are consistent with NIST Special Publication 800-48 and address usage, implementation, monitoring, and authorization of wireless technologies.</p>		✓	✓
AC-18.3	<p><i>Examine</i> organizational records or documents to determine if the organization tracks and monitors wireless access and usage in accordance with organizational policy and procedures.</p>		✓	✓
AC-18.4	<p><i>Examine</i> organizational records or documents to determine if wireless users have been authorized to access the information system.</p>		✓	✓
AC-18.5	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the wireless access restrictions control is implemented.</p>		✓	✓
AC-18.6	<p><i>Test</i> 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.</p>			✓
AC-18.7	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently employs wireless access restrictions on an ongoing basis.</p>			✓
AC-18.8	<p><i>Interview</i> selected organizational personnel with access control responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the wireless access restrictions control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AC-18 WIRELESS ACCESS RESTRICTIONS Control Enhancement: (1) The organization uses authentication and encryption to protect wireless access to the information system.		✓	✓
AC-18.9	<i>Examine the configuration of the information system to determine if wireless access to the system is only permitted through the use of authentication with encryption.</i>		✓	✓
AC-18.10	<i>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.</i>			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES <u>Control:</u> 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.</p>		✓	✓
AC-19.1	<p><i>Examine organizational records or documents to determine if: (i) the organization establishes and documents restrictions and implementation guidance for portable and mobile devices; (ii) the organization monitors and controls the use of portable and mobile devices; and (iii) appropriate organizational officials authorize the use of portable and mobile devices and device access to organizational information systems.</i></p>		✓	✓
AC-19.2	<p><i>Interview selected organizational personnel with access to the information system and examine organizational records or documents detailing the use of portable and mobile devices to determine if personnel are complying with the usage restrictions and applying the implementation guidance on the use of portable and mobile devices in accordance with organization policy and procedures.</i></p>		✓	✓
AC-19.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control for portable and mobile devices is implemented.</i></p>		✓	✓
AC-19.4	<p><i>Test the 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.</i></p>			✓
AC-19.5	<p><i>Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently implements access controls for portable and mobile devices on an ongoing basis.</i></p>			✓
AC-19.6	<p><i>Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access control for portable and mobile devices are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES Control Enhancement: (1) The organization employs removable hard drives or cryptography to protect information residing on portable and mobile devices.		✓	✓
AC-19.7	<i>Examine</i> organizational records or documents to determine if the organization employs removable hard drives or cryptography to protect information on portable and mobile devices.		✓	✓
AC-19.8	<i>Interview</i> 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.			✓
AC-19.9	<i>Examine</i> selected authorized portable or mobile devices to determine if the devices employ removable hard drives or cryptography to protect the information on the devices.			✓

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AC-20 PERSONALLY OWNED INFORMATION SYSTEMS</p> <p><u>Control:</u> 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.</p>	✓	✓	✓
AC-20.1	<p><i>Examine 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 malicious code 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, malicious code definitions, firewall version updates, malicious code protection definitions).</i></p>	✓	✓	✓
AC-20.2	<p><i>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.</i></p>	✓	✓	✓
AC-20.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personally owned information systems control is implemented.</i></p>		✓	✓
AC-20.4	<p><i>Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if the organization consistently employs restrictions on the use of personally owned information system on an ongoing basis.</i></p>			✓
AC-20.5	<p><i>Interview selected organizational personnel with access control responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personally owned information systems control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

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

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES <u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	✓	✓	✓
AT-1.1	<i>Examine</i> organizational records or documents to determine if security awareness and training 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.	✓	✓	✓
AT-1.2	<i>Examine</i> the security awareness and training policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	✓	✓	✓
AT-1.3	<i>Examine</i> the security awareness and training procedures to determine if the procedures are sufficient to address all areas identified in the security awareness and training policy and all associated security awareness and training controls.		✓	✓
AT-1.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security awareness and training policy and procedures control is implemented.		✓	✓
AT-1.5	<i>Examine</i> the security awareness and training policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance.			✓
AT-1.6	<i>Interview</i> selected organizational personnel with security awareness and training responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies the awareness and training policy and procedures on an ongoing basis.			✓
AT-1.7	<i>Interview</i> selected organizational personnel with security awareness and training responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security awareness and training policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: AWARENESS AND TRAINING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AT-2 SECURITY AWARENESS</p> <p><u>Control:</u> The organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and [<i>Assignment: organization-defined frequency, at least annually</i>] thereafter.</p>	✓	✓	✓
AT-2.1	<p><i>Examine</i> organizational records or documents to determine if: (i) security awareness instruction is provided to all users; (ii) records include the type of instruction received and the date completed; and (iii) initial and refresher instruction is provided in accordance with organization-defined frequency, at least annually.</p>	✓	✓	✓
AT-2.2	<p><i>Examine</i> security awareness instructional materials to determine if the materials address the specific requirements of the organization and the information systems to which personnel have authorized access.</p>		✓	✓
AT-2.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security awareness control is implemented.</p>		✓	✓
AT-2.4	<p><i>Interview</i> selected organizational personnel with security awareness and training responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts security awareness instruction on an ongoing basis.</p>			✓
AT-2.5	<p><i>Interview</i> selected organizational personnel with security awareness and training responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security awareness control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: AWARENESS AND TRAINING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AT-3 SECURITY TRAINING <u>Control:</u> The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system and [Assignment: organization-defined frequency] thereafter.</p>	✓	✓	✓
AT-3.1	<p><i>Examine</i> organizational records or documents to determine if the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities.</p>	✓	✓	✓
AT-3.2	<p><i>Examine</i> organizational records or documents to determine if: (i) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system; (ii) records include the type of security training received and the date completed; and (iii) the organization provides initial and refresher training in accordance with organization-defined frequency.</p>	✓	✓	✓
AT-3.3	<p><i>Examine</i> the security training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities.</p>		✓	✓
AT-3.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security training control is implemented.</p>		✓	✓
AT-3.5	<p><i>Interview</i> selected organizational personnel with security awareness and training responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts security training on an ongoing basis.</p>			✓
AT-3.6	<p><i>Interview</i> selected organizational personnel with security awareness and training responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security training control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: AWARENESS AND TRAINING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AT-4 SECURITY TRAINING RECORDS <u>Control:</u> The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.</p>	✓	✓	✓
AT-4.1	<p><i>Examine</i> organizational records or documents to determine if the organization monitors and fully documents basic security awareness training and specific information system security training.</p>	✓	✓	✓
AT-4.2	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security training records control is implemented.</p>		✓	✓
AT-4.3	<p><i>Interview</i> selected organizational personnel with security awareness and training responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently monitors and documents security training activities on an ongoing basis.</p>			✓
AT-4.4	<p><i>Interview</i> selected organizational personnel with security awareness and training responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security training records control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: AWARENESS AND TRAINING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS <u>Control:</u> The organization establishes and maintains contacts with special interest groups, specialized forums, or professional associations to stay up to date with the latest recommended security practices, techniques, and technologies.</p>			
AT-5.1	<p><i>Examine organizational records or documents to determine if the organization establishes and maintains contact with special interest groups, specialized forums, or professional associations to keep currency with state-of-the-practice security techniques and technologies.</i></p>			
AT-5.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contacts with security groups and associations control is implemented.</i></p>			
AT-5.3	<p><i>Interview selected organizational personnel with security awareness and training responsibilities and examine organizational records or documents to determine if the organization consistently establishes and maintains contacts with relevant security groups and associations on an ongoing basis.</i></p>			

ASSESSMENT PROCEDURES

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES <u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	✓	✓	✓
AU-1.1	<i>Examine organizational records or documents to determine if audit and accountability 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.</i>	✓	✓	✓
AU-1.2	<i>Examine the audit and accountability policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</i>	✓	✓	✓
AU-1.3	<i>Examine the audit and accountability procedures to determine if the procedures are sufficient to address all areas identified in the audit and accountability policy and all associated audit and accountability controls.</i>		✓	✓
AU-1.4	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit and accountability policy and procedures control is implemented.</i>		✓	✓
AU-1.5	<i>Examine the audit and accountability policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance.</i>			✓
AU-1.6	<i>Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if the organization consistently applies the audit and accountability policy and procedures on an ongoing basis.</i>			✓
AU-1.7	<i>Interview selected organizational personnel with audit and accountability responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit and accountability policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AU-2 AUDITABLE EVENTS <u>Control:</u> The information system generates audit records for the following events: [Assignment: organization-defined auditable events].	✓	✓	✓
AU-2.1	<i>Examine</i> organizational records or documents and the information system configuration settings to determine if the system generates audit records for the organization-defined auditable events.	✓	✓	✓
AU-2.2	<i>Test</i> the information system by attempting to perform actions that are configured to generate an audit record.		✓	✓
AU-2.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the auditable events control is implemented.		✓	✓
AU-2.4	<i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently generates audit records for auditable events on an ongoing basis.			✓
AU-2.5	<i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the auditable events control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	AU-2 AUDITABLE EVENTS <u>Control Enhancement:</u> (1) The information system provides the capability to compile audit records from multiple components throughout the system into a system wide (logical or physical), time-correlated audit trail.			
AU-2.6	<i>Interview</i> selected organizational personnel with audit and accountability responsibilities to determine if the information system compiles audit records into a system wide (logical or physical), time-correlated audit trail.			
AU-2.7	<i>Examine</i> the information system audit trail to determine if the system accurately compiles audit records from multiple components.			
AU-2.8	<i>Test</i> the information system audit trail to determine if it accurately compiles audit records from multiple components by artificially launching auditable events that are configured to generate audit records assigned to different component collection points.			

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AU-2 AUDITABLE EVENTS Control Enhancement: (2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.</p>			
AU-2.9	<p><i>Examine organizational records or documents to determine if the information system provides the capability to manage the selection of events to be audited by individual components of the system.</i></p>			
AU-2.10	<p><i>Test the capability of information system to manage the selection of events to be audited by configuring different sets of events to be audited by artificially launching auditable events that are configured to generate audit records for the selected events and ensuring they indeed generate audit records.</i></p>			

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AU-3 CONTENT OF AUDIT RECORDS <u>Control:</u> The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.</p>	✓	✓	✓
AU-3.1	<p><i>Examine</i> organizational records or documents to determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.</p>	✓	✓	✓
AU-3.2	<p><i>Test</i> the content of audit records by attempting to perform actions that are configured to generate audit records to determine if the audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.</p>		✓	✓
AU-3.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the content of audit records control is implemented.</p>		✓	✓
AU-3.4	<p><i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently captures sufficient audit information to support organizational audit and accountability requirements on an ongoing basis.</p>			✓
AU-3.5	<p><i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the content of audit records control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>AU-3 CONTENT OF AUDIT RECORDS <u>Control Enhancement:</u> (1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.</p>		✓	✓
AU-3.6	<p><i>Examine</i> organizational records or documents to determine if the information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.</p>		✓	✓

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
AU-3.7	<i>Test the information system capability to include additional, more detailed information in the audit records for audit events by changing the audit configuration settings to add additional information and by performing actions that create audit records to ensure the additional information is captured.</i>		✓	✓
	<p>AU-3 CONTENT OF AUDIT RECORDS <u>Control Enhancement:</u> (2) The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.</p>			✓
AU-3.8	<i>Examine organizational records or documents to determine if the information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.</i>			✓
AU-3.9	<i>Test the information system capability to determine if the content of audit records generated by individual components throughout the system are centrally managed by artificially generating auditable events at different components and utilizing the central management functionality.</i>			✓

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AU-4 AUDIT STORAGE CAPACITY <u>Control:</u> The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.</p>	✓	✓	✓
AU-4.1	<p><i>Examine</i> the information system configuration to determine if the organization allocates sufficient audit record storage capacity and establishes configuration settings to prevent such capacity from being exceeded.</p>	✓	✓	✓
AU-4.2	<p><i>Test</i> the information system configuration to determine if the organization allocates sufficient audit record storage capacity and establishes configuration settings to prevent such capacity from being exceeded by artificially generating enough auditable events to create a number of audit records to exceed the storage capacity.</p>		✓	✓
AU-4.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit storage capacity control is implemented.</p>		✓	✓
AU-4.4	<p><i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently allocates sufficient audit storage capacity on an ongoing basis.</p>			✓
AU-4.5	<p><i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit storage capacity control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AU-5 AUDIT PROCESSING <u>Control:</u> In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	✓	✓	✓
AU-5.1	<i>Examine</i> the information system configuration to determine if in the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes any additional organization-defined actions.	✓	✓	✓
AU-5.2	<i>Test</i> the information system configuration to determine in the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes any additional organization-defined actions by artificially generating auditable events to cause an audit failure or excess capacity condition.		✓	✓
AU-5.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit processing control is implemented.		✓	✓
AU-5.4	<i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently handles audit processing anomalies including audit failures and exceeding storage capacity on an ongoing basis.			✓
AU-5.5	<i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit processing control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	AU-5 AUDIT PROCESSING <u>Control Enhancement:</u> (1) The information system provides a warning when allocated audit record storage volume reaches [Assignment: organization-defined percentage of maximum audit record storage capacity].			✓
AU-5.6	<i>Examine</i> organizational records or documents and the information system configuration to determine if the system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity.			✓

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

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
AU-5.7	<i>Test the information system configuration to determine if the system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity by artificially generating auditable events to cause an excess capacity condition.</i>			✓

Draft

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING <u>Control:</u> The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.</p>		✓	✓
AU-6.1	<p><i>Examine</i> organizational records or documents to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.</p>		✓	✓
AU-6.2	<p><i>Test</i> the audit monitoring, analysis and reporting process to determine if the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions by artificially generating auditable events to cause an audit failure or suspicious activity condition and monitoring how the organization reacts.</p>		✓	✓
AU-6.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit monitoring, analysis, and reporting control is implemented.</p>		✓	✓
AU-6.4	<p><i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts audit monitoring, analysis, and reporting on an ongoing basis.</p>			✓
AU-6.5	<p><i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit monitoring, analysis, and reporting control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING <u>Control Enhancement:</u> (1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.</p>			✓
AU-6.6	<p><i>Examine</i> organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.</p>			✓

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
AU-6.7	<i>Test the information system configuration to determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities by artificially generating auditable events and monitoring the results.</i>			✓
	AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING <u>Control Enhancement:</u> (2) The organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.			
AU-6.8	<i>Examine organizational records or documents and the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.</i>			
AU-6.9	<i>Test the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications by artificially generating auditable events and monitoring the results.</i>			

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AU-7 AUDIT REDUCTION AND REPORT GENERATION <u>Control:</u> The information system provides an audit reduction and report generation capability.</p>		✓	✓
AU-7.1	<p><i>Examine</i> the information system configuration to determine if the system provides an audit reduction and report generation capability.</p>		✓	✓
AU-7.2	<p><i>Test</i> the audit reduction and report generation capability by artificially generating a sufficient number of auditable events to cause an audit reduction and report generation condition.</p>		✓	✓
AU-7.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit reduction and report generation control is implemented.</p>		✓	✓
AU-7.4	<p><i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently provides an audit reduction and report generation capability on an ongoing basis.</p>			✓
AU-7.5	<p><i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit reduction and report generation control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>AU-7 AUDIT REDUCTION AND REPORT GENERATION <u>Control Enhancement:</u> (1) The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.</p>			✓
AU-7.6	<p><i>Examine</i> organizational records or documents and the information system configuration to determine if the system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.</p>			✓
AU-7.7	<p><i>Test</i> the information system configuration to determine if the system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria by artificially generating auditable events based on selected event criteria.</p>			✓

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AU-8 TIME STAMPS <u>Control:</u> The information system provides time stamps for use in audit record generation.		✓	✓
AU-8.1	<i>Examine</i> the information system configuration to determine if the system provides time stamps for use in audit record generation.		✓	✓
AU-8.2	<i>Test</i> the use of time stamps within the audit record generation capability of the information system by artificially generating an auditable event at a known time and compare the time stamp on the resulting audit record.		✓	✓
AU-8.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the time stamps control is implemented.		✓	✓
AU-8.4	<i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently provides time stamps on an ongoing basis.			✓
AU-8.5	<i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the time stamps control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	AU-9 PROTECTION OF AUDIT INFORMATION <u>Control</u> : The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	✓	✓	✓
AU-9.1	<i>Examine</i> the information system configuration to determine if the system protects audit information and audit tools from unauthorized access, modification, and deletion.	✓	✓	✓
AU-9.2	<i>Test</i> the protection of audit information and audit tools from unauthorized access, modification, and deletion by attempting to gain unauthorized access, modify, and delete audit information.		✓	✓
AU-9.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the protection of audit information control is implemented.		✓	✓
AU-9.4	<i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently protects audit information on an ongoing basis.			✓
AU-9.5	<i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the protection of audit information control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	AU-9 PROTECTION OF AUDIT INFORMATION <u>Control Enhancement</u> : (1) The information system produces audit information on hardware-enforced, write-once media.			
AU-9.6	<i>Examine</i> organizational records or documents and the information system configuration to determine if the system produces audit information on hardware-enforced, write-once media.			
AU-9.7	<i>Test</i> the information system to determine if it produces audit information on hardware-enforced, write-once media by executing the process to create the audit information on a write-once media.			

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AU-10 NON-REPUDIATION</p> <p><u>Control:</u> The information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).</p>			
AU-10.1	<p><i>Examine</i> the information system configuration to determine if the system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).</p>			
AU-10.2	<p><i>Test</i> the information system’s non-repudiation capability by: (i) demonstrating that when the non-repudiation capability is applied to a “test” action (e.g., create information, send a message, approve information[e.g., to indicate concurrence or sign a contract]), the organization can determine whether a given individual took the particular action and, when applicable, whether a given individual received something as a result of the action (e.g., received a message as a result of the action); and (ii) by demonstrating that it is not possible to alter or spoof the responsible individual’s identity for a given action.</p>			
AU-10.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the non-repudiation control is implemented.</p>			
AU-10.4	<p><i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently provides a non-repudiation capability on an ongoing basis.</p>			
AU-10.5	<p><i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the non-repudiation control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			

FAMILY: AUDIT AND ACCOUNTABILITY

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>AU-11 AUDIT RETENTION</p> <p><u>Control:</u> The organization retains audit logs for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.</p>	✓	✓	✓
AU-11.1	<p><i>Examine</i> organizational records or documents to determine if the organization retains information system audit logs for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.</p>	✓	✓	✓
AU-11.2	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the audit retention control is implemented.</p>		✓	✓
AU-11.3	<p><i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently retains audit information on an ongoing basis.</p>			✓
AU-11.4	<p><i>Interview</i> selected organizational personnel with audit and accountability responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the audit retention control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

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

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CA-1 CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES</p> <p><u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, 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.</p>	✓	✓	✓
CA-1.1	<p><i>Examine organizational records or documents to determine if security assessment, certification, and accreditation 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.</i></p>	✓	✓	✓
CA-1.2	<p><i>Examine the security assessment, certification, and accreditation policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</i></p>	✓	✓	✓
CA-1.3	<p><i>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 policy and all associated security assessment, certification, and accreditation controls.</i></p>		✓	✓
CA-1.4	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security assessment, certification, and accreditation policies and procedures control is implemented.</i></p>		✓	✓
CA-1.5	<p><i>Examine the security assessment, certification, and accreditation policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance.</i></p>			✓
CA-1.6	<p><i>Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if the organization consistently applies the security assessment, certification, and accreditation policy and procedures on an ongoing basis.</i></p>			✓

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
CA-1.7	<p><i>Interview selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security assessment, certification, and accreditation control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

Draft

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CA-2 SECURITY ASSESSMENTS</p> <p><u>Control:</u> The organization conducts an assessment of the security controls in the information system [<i>Assignment: organization-defined frequency, at least annually</i>] 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.</p>		✓	✓
CA-2.1	<p><i>Examine</i> organizational records or documents 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 organization-defined frequency.</p>		✓	✓
CA-2.2	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security assessments control is implemented.</p>		✓	✓
CA-2.3	<p><i>Interview</i> selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and <i>examine</i> organizational records or documents to determine if the organization assesses security controls in the information system on an ongoing basis.</p>			✓
CA-2.4	<p><i>Interview</i> selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security assessments control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CA-3 INFORMATION SYSTEM CONNECTIONS <u>Control:</u> The organization authorizes all interconnections 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.</p>	✓	✓	✓
CA-3.1	<p><i>Examine</i> organizational records or documents to determine if all external information systems (i.e., information systems outside of the accreditation boundary that are connected to the information system) are identified and all resulting system connections are authorized and approved by appropriate organizational officials.</p>	✓	✓	✓
CA-3.2	<p><i>Examine</i> information system connection agreements to determine if the agreements are consistent with NIST Special Publication 800-47.</p>	✓	✓	✓
CA-3.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system connections control is implemented.</p>		✓	✓
CA-3.4	<p><i>Interview</i> selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently authorizes, monitors, and controls information system connections on an ongoing basis.</p>			✓
CA-3.5	<p><i>Interview</i> selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information systems connection control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CA-4 SECURITY CERTIFICATION <u>Control:</u> 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.</p>	✓	✓	✓
CA-4.1	<p><i>Examine</i> organizational records or documents to determine if a security certification process is defined that assesses the effectiveness of each security control in the information system for correct implementation, intended operation, and producing the desired outcome with respect to meeting the security requirements for the system.</p>	✓	✓	✓
CA-4.2	<p><i>Examine</i> organizational records or documents to determine if the organization employs a security certification process in accordance with NIST Special Publications 800-37 and 800-53A.</p>	✓	✓	✓
CA-4.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security certification control is implemented.</p>		✓	✓
CA-4.4	<p><i>Interview</i> selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts security certifications on an ongoing basis.</p>			✓
CA-4.5	<p><i>Interview</i> selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security certification control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>CA-4 SECURITY CERTIFICATION <u>Control Enhancement:</u> (1) The assessment of the security controls in the information system for purposes of security certification is conducted by an independent certification agent or certification team.</p>		✓	✓
CA-4.6	<p><i>Examine</i> organizational records or documents to determine if an independent certification agent or certification team conducts the security certification of the information system.</p>		✓	✓

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CA-5 PLAN OF ACTION AND MILESTONES <u>Control:</u> The organization develops and updates [<i>Assignment: organization-defined frequency</i>], 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.</p>	✓	✓	✓
CA-5.1	<p><i>Examine</i> organizational records or documents to determine if a plan of action and milestones for the information system: (i) exists; (ii) is documented; and (iii) is updated in accordance with organization-defined frequency.</p>	✓	✓	✓
CA-5.2	<p><i>Examine</i> the plan of action and milestones 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 information system.</p>	✓	✓	✓
CA-5.3	<p><i>Examine</i> organizational records or documents to determine if the organization follows the plan of action and milestones (i.e., correcting deficiencies and meeting milestones).</p>		✓	✓
CA-5.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the plan of action and milestones control is implemented.</p>		✓	✓
CA-5.5	<p><i>Interview</i> selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently develops and updates a plan of action and milestones for the information system on an ongoing basis.</p>			✓
CA-5.6	<p><i>Interview</i> selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the plan of action and milestones control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CA-6 SECURITY ACCREDITATION <u>Control:</u> The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [Assignment: organization-defined frequency, at least every three years]. A senior organizational official signs and approves the security accreditation.</p>	✓	✓	✓
CA-6.1	<p><i>Examine</i> organizational records or documents to determine if a security 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.</p>	✓	✓	✓
CA-6.2	<p><i>Examine</i> organizational records or documents to determine if the security accreditation process employed by the organization is consistent with NIST Special Publications 800-37.</p>	✓	✓	✓
CA-6.3	<p><i>Examine</i> organizational records or documents to determine if a senior organizational official signs and approves the security accreditation.</p>	✓	✓	✓
CA-6.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security accreditation control is implemented.</p>		✓	✓
CA-6.5	<p><i>Interview</i> selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts security accreditations on an ongoing basis.</p>			✓
CA-6.6	<p><i>Interview</i> selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security accreditation control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CA-7 CONTINUOUS MONITORING <u>Control:</u> The organization monitors the security controls in the information system on an ongoing basis.</p>	✓	✓	✓
CA-7.1	<p><i>Examine</i> organizational records or documents to determine if the organization monitors the security controls in the information system on an ongoing basis.</p>	✓	✓	✓
CA-7.2	<p><i>Examine</i> organizational records or documents to determine if the organization employs a security control monitoring process consistent with NIST Special Publications 800-37 and 800-53A.</p>	✓	✓	✓
CA-7.3	<p><i>Examine</i> organizational records or documents to determine if the organization: (i) assesses designated security controls in the information system; (ii) analyzes for impact, documents, and reports changes to or deficiencies in the operation of the security controls; and (iii) makes adjustments to the information system security plan and plan of action and milestones, as appropriate.</p>		✓	✓
CA-7.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the continuous monitoring control is implemented.</p>		✓	✓
CA-7.5	<p><i>Interview</i> selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently monitors the security controls in the information system on an ongoing basis.</p>			✓
CA-7.6	<p><i>Interview</i> selected organizational personnel with security assessment, certification, and/or accreditation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the continuous monitoring control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

ASSESSMENT PROCEDURES**FAMILY:** CONFIGURATION MANAGEMENT**CLASS:** OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES <u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.</p>	✓	✓	✓
CM-1.1	<p><i>Examine</i> organizational records or documents to determine if the configuration management 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.</p>	✓	✓	✓
CM-1.2	<p><i>Examine</i> the configuration management policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</p>	✓	✓	✓
CM-1.3	<p><i>Examine</i> the configuration management procedures to determine if the procedures are sufficient to address all areas identified in the configuration management policy and all associated configuration management controls.</p>		✓	✓
CM-1.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration management policies and procedures control is implemented.</p>		✓	✓
CM-1.5	<p><i>Examine</i> the configuration management policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance.</p>			✓
CM-1.6	<p><i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies the configuration management policy and procedures on an ongoing basis.</p>			✓
CM-1.7	<p><i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the configuration management policies and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: CONFIGURATION MANAGEMENT

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	CM-2 BASELINE CONFIGURATION AND SYSTEM COMPONENT INVENTORY <u>Control:</u> The organization develops, documents, and maintains a current, baseline configuration of the information system, an inventory of the system's constituent components, and relevant ownership information.	✓	✓	✓
CM-2.1	<i>Examine</i> organizational records or documents to determine if the organization develops, documents, and maintains a baseline configuration of the information system which includes key architectural components and the relationship among those components.	✓	✓	✓
CM-2.2	<i>Examine</i> organizational records or documents to determine if the organization develops, documents, and maintains an inventory of the hardware, software, and firmware components that compose the information system and ownership information by component.	✓	✓	✓
CM-2.3	<i>Examine</i> organizational records or documents to determine if the inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture).		✓	✓
CM-2.4	<i>Examine</i> organizational records or documents to determine if the inventory of information system components designates those components required to implement and/or conduct contingency operations.		✓	✓
CM-2.5	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the baseline configuration and system component inventory control is implemented.		✓	✓
CM-2.6	<i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently manages the baseline configuration and component inventory of the information system on an ongoing basis.			✓
CM-2.7	<i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the baseline configuration and system component inventory control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: CONFIGURATION MANAGEMENT

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CM-2 BASELINE CONFIGURATION AND SYSTEM COMPONENT INVENTORY <u>Control Enhancement:</u> (1) The organization updates the baseline configuration of the information system and inventory of system components as an integral part of information system component installations.</p>		✓	✓
CM-2.8	<p><i>Examine organizational records or documents to determine if the organization identifies: (i) instances that trigger baseline configuration and component inventory updates; (ii) the frequency of updates to the baseline configuration and component inventory; (iii) the dates of baseline configuration and inventory updates, a summary of the updates, and the name of the individuals performing the updates.</i></p>		✓	✓
	<p>CM-2 BASELINE CONFIGURATION AND SYSTEM COMPONENT INVENTORY <u>Control Enhancement:</u> (2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system and inventory of information system components.</p>			✓
CM-2.9	<p><i>Examine organizational records or documents to determine if the organization employs automated mechanisms to manage the information system baseline configuration and system component inventory functions.</i></p>			✓
CM-2.10	<p><i>Test the automated mechanism(s) within the information system to determine if each automated function is properly configured to ensure that baseline configuration and system component inventory updates are scheduled and conducted as required.</i></p>			✓
CM-2.11	<p><i>Examine organizational records or documents to determine if the log of baseline configuration and system component inventory updates for the information system is up-to-date, accurate, complete, and available to appropriate organizational personnel.</i></p>			✓

FAMILY: CONFIGURATION MANAGEMENT

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CM-3 CONFIGURATION CHANGE CONTROL</p> <p><u>Control</u>: The organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.</p>		✓	✓
CM-3.1	<i>Examine</i> organizational records or documents to determine if the organization documents and controls changes to the information system.		✓	✓
CM-3.2	<i>Examine</i> organizational records or documents to determine if appropriate organizational officials approve information system changes in accordance with organizational policy and procedures.		✓	✓
CM-3.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration change control is implemented.		✓	✓
CM-3.4	<i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently documents and controls information system configuration changes on an ongoing basis.			✓
CM-3.5	<i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the configuration change control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	<p>CM-3 CONFIGURATION CHANGE CONTROL</p> <p><u>Control Enhancement</u>:</p> <p>(1) The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.</p>			✓
CM-3.6	<i>Examine</i> organizational records or documents to determine if the organization employs automated mechanisms to manage configuration changes to the information system			✓
CM-3.7	<i>Test</i> the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.			✓

FAMILY: CONFIGURATION MANAGEMENT

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	CM-4 MONITORING CONFIGURATION CHANGES <u>Control:</u> The organization monitors changes to the information system and conducts security impact analyses to determine the effects of the changes.		✓	✓
CM-4.1	<i>Examine</i> organizational records or documents to determine if the organization monitors changes to the information system and identifies the types of changes monitored.		✓	✓
CM-4.2	<i>Examine</i> organizational records or documents to determine if the organization performs security impact analyses to assess the effects of changes to the information system.		✓	✓
CM-4.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the monitoring configuration changes control is implemented.		✓	✓
CM-4.4	<i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently monitors configuration changes to the information system on an ongoing basis.			✓
CM-4.5	<i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the monitoring configuration changes control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: CONFIGURATION MANAGEMENT

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CM-5 ACCESS RESTRICTIONS FOR CHANGE</p> <p><u>Control:</u> The organization enforces physical and logical access restrictions associated with changes to the information system and generates, retains, and reviews records reflecting all such changes.</p>		✓	✓
CM-5.1	<p><i>Examine</i> organizational records or documents to determine if the organization maintains a list of personnel authorized to access the information system for purposes of initiating changes, upgrades, and/or modifications to the system.</p>		✓	✓
CM-5.2	<p><i>Examine</i> organizational records or documents to determine if the organization enforces physical and logical access restrictions associated with changes to the information system and generates, retains, and reviews records reflecting all such changes.</p>		✓	✓
CM-5.3	<p><i>Examine</i> organizational records or documents identifying changes made to the information system to determine if only authorized personnel initiated, tested, approved, and implemented changes to the system.</p>		✓	✓
CM-5.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access restrictions for change control is implemented.</p>		✓	✓
CM-5.5	<p><i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently enforces physical and logical access to the information system for purposes of change control on an ongoing basis.</p>			✓
CM-5.6	<p><i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access restrictions for change control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>CM-5 ACCESS RESTRICTIONS FOR CHANGE</p> <p><u>Control Enhancement:</u></p> <p>(1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.</p>			✓
CM-5.7	<p><i>Examine</i> organizational records or documents to determine if the organization employs automated mechanisms to enforce access restrictions and to support auditing of the enforcement of actions.</p>			✓
CM-5.8	<p><i>Test</i> the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to enforce access restrictions and to support auditing of the enforcement of actions.</p>			✓

FAMILY: CONFIGURATION MANAGEMENT**CLASS:** OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
CM-5.9	<i>Examine</i> organizational records or documents to determine if the organization: (i) restricts access to automated mechanism(s) to authorized employees only; and (ii) tracks all activities performed by employees using the automated mechanism(s) to support auditing of the enforcement actions.			✓

Draft

FAMILY: CONFIGURATION MANAGEMENT

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CM-6 CONFIGURATION SETTINGS <u>Control:</u> The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.</p>	✓	✓	✓
CM-6.1	<p><i>Examine</i> organizational records or documents to determine if the organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.</p>	✓	✓	✓
CM-6.2	<p><i>Examine</i> selected information system configuration settings to determine if they are configured in accordance with the organization-defined settings.</p>		✓	✓
CM-6.3	<p><i>Examine</i> organization documentation or records to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the configuration settings control is implemented.</p>		✓	✓
CM-6.4	<p><i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies configuration settings to the information system on an ongoing basis.</p>			✓
CM-6.5	<p><i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the configuration settings control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>CM-6 CONFIGURATION SETTINGS <u>Control Enhancement:</u> (1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.</p>			✓
CM-6.6	<p><i>Examine</i> organizational records or documents to determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.</p>			✓
CM-6.7	<p><i>Examine</i> output generated by the information system to determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.</p>			✓

FAMILY: CONFIGURATION MANAGEMENT**CLASS:** OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
CM-6.8	<i>Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to centrally manage, apply, and verify configuration settings.</i>			✓

Draft

FAMILY: CONFIGURATION MANAGEMENT

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CM-7 LEAST FUNCTIONALITY</p> <p><u>Control:</u> The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services].</p>		✓	✓
CM-7.1	<p><i>Examine</i> organizational records or documents to determine if the information system is configured to provide only essential capabilities and to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services.</p>		✓	✓
CM-7.2	<p><i>Test</i> the information system to determine if the identified functions, ports, protocols, and services are prohibited or restricted.</p>		✓	✓
CM-7.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the least functionality control is implemented.</p>		✓	✓
CM-7.4	<p><i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies the concept of least functionality to the information system on an ongoing basis.</p>			✓
CM-7.5	<p><i>Interview</i> selected organizational personnel with configuration management responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the least functionality control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>CM-7 LEAST FUNCTIONALITY</p> <p><u>Control Enhancement:</u></p> <p>(1) The organization reviews the information system [Assignment: organization-defined frequency], to identify and eliminate unnecessary functions, ports, protocols, and/or services.</p>			✓
CM-7.6	<p><i>Examine</i> organizational records or documents in accordance with organization-defined frequency to determine if the organization reviews the information system to identify and eliminate unnecessary functions, ports, protocols, and/or services.</p>			✓

ASSESSMENT PROCEDURES

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES</p> <p><u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.</p>	✓	✓	✓
CP-1.1	<p><i>Examine</i> organizational records or documents 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.</p>	✓	✓	✓
CP-1.2	<p><i>Examine</i> the contingency planning policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</p>	✓	✓	✓
CP-1.3	<p><i>Examine</i> 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.</p>		✓	✓
CP-1.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency planning policy and procedures control is implemented.</p>		✓	✓
CP-1.5	<p><i>Examine</i> 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.</p>			✓
CP-1.6	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies the contingency planning policy and procedures on an ongoing basis.</p>			✓
CP-1.7	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency planning policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-2 CONTINGENCY PLAN</p> <p><u>Control:</u> 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.</p>	✓	✓	✓
CP-2.1	<p><i>Examine</i> organizational records or documents to determine if a contingency plan: (i) exists; (ii) is documented; (iii) is disseminated to appropriate elements within the organization; and (iv) is reviewed and approved by responsible officials within the organization.</p>	✓	✓	✓
CP-2.2	<p><i>Examine</i> the contingency plan for the information system to determine if the plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system consistent with NIST Special Publication 800-34.</p>	✓	✓	✓
CP-2.3	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities to determine if key operating elements within the organization understand the contingency plan and are ready to implement the plan.</p>		✓	✓
CP-2.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan control is implemented.</p>		✓	✓
CP-2.5	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if designated officials within the organization consistently review and approve the contingency plan and distribute the plan to key contingency personnel on an ongoing basis.</p>			✓
CP-2.6	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency plan control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-2 CONTINGENCY PLAN</p> <p><u>Control Enhancement:</u></p> <p>(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).</p>		✓	✓
CP-2.7	<p><i>Examine organizational records or documents to determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan) and if the contingency plan supports the requirements in the related plans.</i></p>		✓	✓

Draft

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-3 CONTINGENCY TRAINING</p> <p><u>Control</u>: 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].</p>		✓	✓
CP-3.1	<i>Examine</i> organizational records or documents to determine if the organization identifies personnel with significant contingency roles and responsibilities and documents those roles and responsibilities.		✓	✓
CP-3.2	<i>Examine</i> organizational records or documents to determine if the organization: (i) provides contingency training to personnel with significant contingency roles and responsibilities or personnel implementing the contingency plan; (ii) records the type of contingency training received and the date completed; and (iii) provides initial and refresher training in accordance with organization-defined frequency, at least annually.		✓	✓
CP-3.3	<i>Examine</i> the contingency training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities.		✓	✓
CP-3.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency training control is implemented.		✓	✓
CP-3.5	<i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts contingency training on an ongoing basis.			✓
CP-3.6	<i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency training control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	<p>CP-3 CONTINGENCY TRAINING</p> <p><u>Control Enhancement</u>:</p> <p>(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.</p>			✓
CP-3.7	<i>Examine</i> organizational records or documents to determine if the organization simulates contingency training events.			✓
CP-3.8	<i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities to determine how the organization uses simulated events to improve the training process.			✓

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
CP-3.9	<i>Test selected simulated events to determine if organizational personnel respond as expected to the simulated crisis situation.</i>			✓
	CP-3 CONTINGENCY TRAINING <u>Control Enhancement:</u> (2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.			
CP-3.10	<i>Examine organizational records or documents to determine if the organization employs automated mechanisms to improve contingency training.</i>			
CP-3.11	<i>Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine how the automated mechanisms improve the training process.</i>			
CP-3.12	<i>Test selected automated mechanisms to determine if the mechanisms are operating as intended.</i>			

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-4 CONTINGENCY PLAN TESTING</p> <p><u>Control:</u> 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.</p>		✓	✓
CP-4.1	<i>Examine</i> organizational records or documents to determine if the organization tests its contingency plan using the organization-defined tests and exercises in accordance with the organization-defined frequency and documents the results of the tests.		✓	✓
CP-4.2	<i>Examine</i> organizational records or documents to determine if the organization reviews the contingency plan test results and takes corrective actions.		✓	✓
CP-4.3	<i>Examine</i> organizational records or documents 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.		✓	✓
CP-4.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan testing control is implemented.		✓	✓
CP-4.5	<i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities to determine the overall effectiveness of the contingency plan and the readiness of the organization to execute the plan.			✓
CP-4.6	<i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts contingency plan testing on an ongoing basis.			✓
CP-4.7	<i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency plan testing control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-4 CONTINGENCY PLAN TESTING <u>Control Enhancement:</u> (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).</p>		✓	✓
CP-4.8	<p><i>Examine organizational records or documents to determine if 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).</i></p>		✓	✓
	<p>CP-4 CONTINGENCY PLAN TESTING <u>Control Enhancement:</u> (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.</p>			✓
CP-4.9	<p><i>Examine organizational records or documents to determine if the organization conducts contingency plan testing at the alternate processing site to familiarize contingency personnel with the facility and its resources and to evaluate the site’s capabilities to support contingency operations.</i></p>			✓
	<p>CP-4 CONTINGENCY PLAN TESTING <u>Control Enhancement:</u> (3) The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.</p>			
CP-4.10	<p><i>Examine organizational records or documents to determine if the organization employs automated mechanisms for contingency testing.</i></p>			
CP-4.11	<p><i>Interview selected organizational personnel with contingency planning and plan implementation responsibilities to determine how the automated mechanisms improve the testing process.</i></p>			
CP-4.12	<p><i>Test selected automated mechanisms to determine if the mechanisms are operating as intended.</i></p>			

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-5 CONTINGENCY PLAN UPDATE</p> <p><u>Control:</u> 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.</p>	✓	✓	✓
CP-5.1	<i>Examine</i> organizational records or documents to determine if the organization updates the contingency plan in accordance with organization-defined frequency, at least annually.	✓	✓	✓
CP-5.2	<i>Examine</i> 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.		✓	✓
CP-5.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency plan update control is implemented.		✓	✓
CP-5.4	<i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently reviews and updates the contingency plan on an ongoing basis.			✓
CP-5.5	<i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the contingency plan update control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-6 ALTERNATE STORAGE SITES <u>Control:</u> The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.</p>		✓	✓
CP-6.1	<p><i>Examine</i> organizational records or documents to determine if alternate storage site agreements are currently in place to permit storage of information system backup information.</p>		✓	✓
CP-6.2	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate storage site control is implemented.</p>		✓	✓
CP-6.3	<p><i>Examine</i> the alternate storage site to determine if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup information.</p>			✓
CP-6.4	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently reviews and updates alternate storage site agreements on an ongoing basis.</p>			✓
CP-6.5	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the alternate storage sites control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>CP-6 ALTERNATE STORAGE SITES <u>Control Enhancement:</u> (1) The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.</p>		✓	✓
CP-6.6	<p><i>Examine</i> the contingency plan to determine if the plan identifies the primary storage site hazards.</p>		✓	✓
CP-6.7	<p><i>Examine</i> the 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 site.</p>		✓	✓

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-6 ALTERNATE STORAGE SITES <u>Control Enhancement:</u> (2) The alternate storage site is configured to facilitate timely and effective recovery operations.</p>			✓
CP-6.8	<p><i>Examine the alternate storage site agreement to determine if the agreement specifies requirements to facilitate timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives).</i></p>			✓
CP-6.9	<p><i>Test the alternate storage site operations to determine if the 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.</i></p>			✓
	<p>CP-6 ALTERNATE STORAGE SITES <u>Control Enhancement:</u> (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.</p>			✓
CP-6.10	<p><i>Examine the 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.</i></p>			✓

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-7 ALTERNATE PROCESSING SITES</p> <p><u>Control</u>: 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.</p>		✓	✓
CP-7.1	<i>Examine</i> organizational records or documents to determine if alternate processing site agreements are currently in place to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.		✓	✓
CP-7.2	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate processing site control is implemented.		✓	✓
CP-7.3	<i>Examine</i> the 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.			✓
CP-7.4	<i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently reviews and updates alternate processing site agreements on an ongoing basis.			✓
CP-7.5	<i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the alternate processing sites control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	<p>CP-7 ALTERNATE PROCESSING SITES</p> <p><u>Control Enhancement</u>:</p> <p>(1) The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards.</p>		✓	✓
CP-7.6	<i>Examine</i> the contingency plan to determine if the plan identifies the primary processing site hazards.		✓	✓
CP-7.7	<i>Examine</i> the 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 site.		✓	✓

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-7 ALTERNATE PROCESSING SITES <u>Control Enhancement:</u> (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.</p>		✓	✓
CP-7.8	<p><i>Examine the 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.</i></p>		✓	✓
	<p>CP-7 ALTERNATE PROCESSING SITES <u>Control Enhancement:</u> (3) Alternate processing site agreements contain priority-of-service provisions in accordance with the organization’s availability requirements.</p>		✓	✓
CP-7.9	<p><i>Examine alternate processing site agreements to determine if the agreements contain priority of service provisions in accordance with the organization’s availability requirements.</i></p>		✓	✓
	<p>CP-7 ALTERNATE PROCESSING SITES <u>Control Enhancement:</u> (4) The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.</p>			✓
CP-7.10	<p><i>Examine alternate processing site agreements to determine if the agreements specify the requirements needed to support the minimum required operational capability of the organization.</i></p>			✓
CP-7.11	<p><i>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.</i></p>			✓

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-8 TELECOMMUNICATIONS SERVICES <u>Control:</u> 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.</p>		✓	✓
CP-8.1	<p><i>Examine</i> alternate telecommunication service agreements 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.</p>		✓	✓
CP-8.2	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the telecommunications services control is implemented.</p>		✓	✓
CP-8.3	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently reviews primary and alternate telecommunications service agreements on an ongoing basis.</p>			✓
CP-8.4	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the telecommunications services control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>CP-8 TELECOMMUNICATIONS SERVICES <u>Control Enhancement:</u> (1) Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements.</p>		✓	✓
CP-8.5	<p><i>Examine</i> primary and alternate telecommunication service agreements to determine if the agreements contain priority of service provisions in accordance with the availability requirements defined in the organization's contingency plan.</p>		✓	✓

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-8 TELECOMMUNICATIONS SERVICES <u>Control Enhancement:</u> (2) Alternate telecommunications services do not share a single point of failure with primary telecommunications services.</p>		✓	✓
CP-8.6	<p><i>Examine primary and alternate telecommunications service agreements and interview appropriate telecommunications service providers to determine if alternate and primary telecommunications services share a single point of failure.</i></p>		✓	✓
	<p>CP-8 TELECOMMUNICATIONS SERVICES <u>Control Enhancement:</u> (3) Alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.</p>			✓
CP-8.7	<p><i>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 site.</i></p>			✓
	<p>CP-8 TELECOMMUNICATIONS SERVICES <u>Control Enhancement:</u> (4) Primary and alternate telecommunications service providers have adequate contingency plans.</p>			✓
CP-8.8	<p><i>Examine the contingency plans from the primary and alternate telecommunication service providers to determine if the contingency plans are adequate.</i></p>			✓

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-9 INFORMATION SYSTEM BACKUP</p> <p><u>Control</u>: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [<i>Assignment: organization-defined frequency</i>] and stores backup information at an appropriately secured location.</p>	✓	✓	✓
CP-9.1	<p><i>Examine</i> organizational records or documents to determine if the organization defines the user-level and system-level information (including system state information) that is required to be backed up and identifies the location for storing backup information.</p>	✓	✓	✓
CP-9.2	<p><i>Examine</i> selected information system backup media, or selected records of backups if available, to determine if the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency and stores the backup information in designated locations in accordance with information system backup procedures.</p>	✓	✓	✓
CP-9.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system backup control is implemented.</p>		✓	✓
CP-9.4	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts information system backups on an ongoing basis.</p>			✓
CP-9.5	<p><i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system backup control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>CP-9 INFORMATION SYSTEM BACKUP</p> <p><u>Control Enhancement</u>:</p> <p>(1) The organization tests backup information [<i>Assignment: organization-defined frequency</i>] to ensure media reliability and information integrity.</p>		✓	✓
CP-9.6	<p><i>Examine</i> organizational records or documents including results from testing of backup operations to determine if the organization conducts testing within the organization-defined frequency, and if the testing results indicate backup media reliability and information integrity.</p>		✓	✓

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-9 INFORMATION SYSTEM BACKUP <u>Control Enhancement:</u> (2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.</p>			✓
CP-9.7	<p><i>Examine organizational records or documents to determine if the organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing and if the use of the backup information contributes to a successful restoration of the identified functions within the information system.</i></p>			✓
	<p>CP-9 INFORMATION SYSTEM BACKUP <u>Control Enhancement:</u> (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.</p>			✓
CP-9.8	<p><i>Examine the storage location for backup copies of the operating system and other critical information system software to determine if the backup copies of the software are stored in a separate facility or in a fire-rated container that is not collocated with the operational software.</i></p>			✓
	<p>CP-9 INFORMATION SYSTEM BACKUP <u>Control Enhancement:</u> (4) The organization encrypts backup information.</p>			
CP-9.9	<p><i>Examine organizational records or documents to determine if copies of backup information are encrypted.</i></p>			
CP-9.10	<p><i>Test the mechanisms used to encrypt backup information on the information system by selectively decrypting selected backup files and comparing the plain text to original backup information.</i></p>			

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION</p> <p><u>Control:</u> 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.</p>	✓	✓	✓
CP-10.1	<i>Examine</i> organizational records or documents to determine if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system.	✓	✓	✓
CP-10.2	<i>Examine</i> organizational records or documents to determine if the organization identifies means for capturing the information system's operational state including all system parameters, patches, configuration settings, and application/system software prior to system disruption or failure.		✓	✓
CP-10.3	<i>Examine</i> organizational records or documents to determine if the organization tests the information system after completion of recovery and reconstitution operations.		✓	✓
CP-10.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system recovery and reconstitution control is implemented.		✓	✓
CP-10.5	<i>Test</i> 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.			✓
CP-10.6	<i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts recovery and reconstitution operations on an ongoing basis.			✓
CP-10.7	<i>Interview</i> selected organizational personnel with contingency planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system recovery and reconstitution control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	<p>CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION</p> <p><u>Control Enhancement:</u></p> <p>(1) The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.</p>			✓
CP-10.8	<i>Examine</i> organizational records or documents including results from contingency plan testing to determine if the organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.			✓

ASSESSMENT PROCEDURES

FAMILY: IDENTIFICATION AND AUTHENTICATION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES <u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	✓	✓	✓
IA-1.1	<i>Examine organizational records or documents to determine if identification and authentication 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.</i>	✓	✓	✓
IA-1.2	<i>Examine the identification and authentication policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</i>	✓	✓	✓
IA-1.3	<i>Examine the identification and authentication procedures to determine if the procedures are sufficient to address all areas identified in the identification and authentication policy and all associated identification and authentication controls.</i>		✓	✓
IA-1.4	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the identification and authentication policy and procedures control is implemented.</i>		✓	✓
IA-1.5	<i>Examine the identification and authentication policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance.</i>			✓
IA-1.6	<i>Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the organization consistently applies the identification and authentication policy and procedures on an ongoing basis.</i>			✓
IA-1.7	<i>Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the identification and authentication policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓

FAMILY: IDENTIFICATION AND AUTHENTICATION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	IA-2 USER IDENTIFICATION AND AUTHENTICATION <u>Control:</u> The information system uniquely identifies and authenticates users (or processes acting on behalf of users).	✓	✓	✓
IA-2.1	<i>Examine</i> organizational records or documents and the information system configuration settings to determine if the system uniquely identifies users and if authentication of user identities is accomplished through the use of passwords, tokens, or biometrics.	✓	✓	✓
IA-2.2	<i>Examine</i> organizational records or documents and the information system configuration settings to determine if passwords, tokens, or biometrics meet Level 1, 2, 3, or 4 requirements consistent with NIST Special Publication 800-63.	✓	✓	✓
IA-2.3	<i>Test</i> the information system to determine if passwords, tokens, or biometrics meet Level 2, 3, or 4 requirements consistent with NIST Special Publication 800-63.		✓	✓
IA-2.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the user identification and authentication control is implemented.		✓	✓
IA-2.5	<i>Examine</i> organizational records or documents to determine if identification and authentication mechanisms are employed at the application level.			✓
IA-2.6	<i>Test</i> the appropriate components within the information system to determine if passwords, tokens, or biometrics meet Level 3 or 4 requirements consistent with NIST Special Publication 800-63.			✓
IA-2.7	<i>Interview</i> selected organizational personnel with identification and authentication responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently identifies and authenticates users on an ongoing basis.			✓
IA-2.8	<i>Interview</i> selected organizational personnel with identification and authentication responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the user identification and authentication control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: IDENTIFICATION AND AUTHENTICATION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	IA-2 USER IDENTIFICATION AND AUTHENTICATION <u>Control Enhancement:</u> (1) The information system employs multifactor authentication.			✓
IA-2.9	<i>Examine organizational records or documents and the information system configuration settings to determine if multifactor authentication is accomplished through some combination of passwords, tokens, or biometrics.</i>			✓
IA-2.10	<i>Test the appropriate components of the information system to determine if a combination of passwords, tokens, or biometrics is used to employ multifactor authentication.</i>			✓

FAMILY: IDENTIFICATION AND AUTHENTICATION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION <u>Control:</u> The information system identifies and authenticates specific devices before establishing a connection.		✓	✓
IA-3.1	<i>Examine</i> organizational records or documents and information system configuration settings to determine if the system uses either shared known information or an organizational authentication solution to identify and authenticate devices on local and/or wide area networks.		✓	✓
IA-3.2	<i>Examine</i> organizational records or documents to determine if the strength of the device authentication mechanism is consistent with the FIPS 199 security categorization of the information system.		✓	✓
IA-3.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the device authentication and authentication control is implemented.		✓	✓
IA-3.4	<i>Test</i> the information system to determine if the system identifies and authenticates specific devices before establishing connections to those devices.			✓
IA-3.5	<i>Interview</i> selected organizational personnel with identification and authentication responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently identifies and authenticates devices prior to establishing connections on an ongoing basis.			✓
IA-3.6	<i>Interview</i> selected organizational personnel with identification and authentication responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the device identification and authentication control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: IDENTIFICATION AND AUTHENTICATION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>IA-4 IDENTIFIER MANAGEMENT</p> <p><u>Control:</u> The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers.</p>	✓	✓	✓
IA-4.1	<p><i>Examine</i> organizational records or documents and information system configuration settings to determine if the organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after an organization-defined time period of inactivity; and (vi) archiving user identifiers.</p>	✓	✓	✓
IA-4.2	<p><i>Examine</i> organizational records or documents to determine if a personal identity verification (PIV) card token is used to uniquely identify and authenticate federal employees and contractors in accordance with FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78.</p>		✓	✓
IA-4.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the identifier management control is implemented.</p>		✓	✓
IA-4.4	<p><i>Interview</i> selected organizational personnel with identification and authentication responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently manages user identifiers for the information system on an ongoing basis.</p>			✓
IA-4.5	<p><i>Interview</i> selected organizational personnel with identification and authentication responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the identifier management control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: IDENTIFICATION AND AUTHENTICATION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>IA-5 AUTHENTICATOR MANAGEMENT</p> <p><u>Control:</u> The organization manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon information system installation.</p>	✓	✓	✓
IA-5.1	<p><i>Examine</i> organizational records or documents and the information system configuration settings to determine if the system protects passwords from unauthorized disclosure and modification when stored and transmitted, prohibits passwords from being displayed when entered, enforces password minimum and maximum lifetime restrictions, and prohibits password reuse for a specified number of generations.</p>	✓	✓	✓
IA-5.2	<p><i>Examine</i> organizational records or documents to determine if the organization establishes administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.</p>	✓	✓	✓
IA-5.3	<p><i>Examine</i> organizational records or documents to determine if the organization changes default authenticators upon information system installation.</p>	✓	✓	✓
IA-5.4	<p><i>Interview</i> selected organizational personnel with identification and authentication responsibilities to determine if users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately.</p>		✓	✓
IA-5.5	<p><i>Examine</i> organizational records or documents to determine if the information system establishes user control of the corresponding private key and maps the authenticated identity to the user account (for PKI-based authentication).</p>		✓	✓
IA-5.6	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the authenticator management control is implemented.</p>		✓	✓
IA-5.7	<p><i>Test</i> the information system to determine if the system protects passwords from unauthorized disclosure and modification when stored and transmitted, prohibits passwords from being displayed when entered, enforces password minimum and maximum lifetime restrictions, and prohibits password reuse for a specified number of generations.</p>			✓

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

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
IA-5.8	<i>Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the organization consistently manages authenticators for the information system on an ongoing basis.</i>			✓
IA-5.9	<i>Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the authenticator management control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓

FAMILY: IDENTIFICATION AND AUTHENTICATION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>IA-6 AUTHENTICATOR FEEDBACK</p> <p><u>Control:</u> The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.</p>	✓	✓	✓
IA-6.1	<p><i>Examine organizational records or documents and information system configuration settings to determine if the system obscures feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password).</i></p>	✓	✓	✓
IA-6.2	<p><i>Test the information system to determine if the feedback provides sufficient information for a legitimate user to understand why access is not granted (e.g., made a keystroke mistake, forgot the password), but does not provide information that would allow an unauthorized user to compromise the authentication mechanism.</i></p>		✓	✓
IA-6.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the authenticator feedback control is implemented.</i></p>		✓	✓
IA-6.4	<p><i>Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the information system consistently obscures feedback of authentication information during the authentication process on an ongoing basis.</i></p>			✓
IA-6.5	<p><i>Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the authenticator feedback control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: IDENTIFICATION AND AUTHENTICATION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION <u>Control:</u> For authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.</p>	✓	✓	✓
IA-7.1	<p><i>Examine organizational records or documents and information system configuration settings to determine if the system employs authentication methods for authentication to a cryptographic module that meet the requirements of FIPS 140-2.</i></p>	✓	✓	✓
IA-7.2	<p><i>Examine organizational records or documents and information system configuration settings to determine if the information system employs authentication methods in accordance with FIPS 201 and NIST Special Publications 800-73 and 800-78 when the cryptographic module is a personal identity verification (PIV) card token.</i></p>	✓	✓	✓
IA-7.3	<p><i>Examine organizational records or documents to determine if the organization clearly documents authentication methods to a cryptographic module for the information system.</i></p>	✓	✓	✓
IA-7.4	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the cryptographic module authentication control is implemented.</i></p>		✓	✓
IA-7.5	<p><i>Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if the organization consistently meets the requirements of FIPS 140-2 for cryptographic module authentication on an ongoing basis.</i></p>			✓
IA-7.6	<p><i>Interview selected organizational personnel with identification and authentication responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the cryptographic module authentication control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

ASSESSMENT PROCEDURES

FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES <u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	✓	✓	✓
IR-1.1	<i>Examine organizational records or documents to determine if 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.</i>	✓	✓	✓
IR-1.2	<i>Examine the incident response policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</i>	✓	✓	✓
IR-1.3	<i>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.</i>		✓	✓
IR-1.4	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response policy and procedures control is implemented.</i>		✓	✓
IR-1.5	<i>Examine the incident response policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance.</i>			✓
IR-1.6	<i>Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if the organization consistently applies incident response policy and procedures on an ongoing basis.</i>			✓
IR-1.7	<i>Interview selected organizational personnel with incident response responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident response policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓

FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>IR-2 INCIDENT RESPONSE TRAINING <u>Control:</u> 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].</p>		✓	✓
IR-2.1	<p><i>Examine</i> organizational records or documents to determine if the organization identifies personnel with significant incident response roles and responsibilities and documents those roles and responsibilities.</p>		✓	✓
IR-2.2	<p><i>Examine</i> organizational records or documents to determine if: (i) incident response training is provided to personnel with significant incident response roles and responsibilities; (ii) records include the type of incident response training received and the date completed; and (iii) initial and refresher training is provided in accordance with organization-defined frequency, at least annually.</p>		✓	✓
IR-2.3	<p><i>Examine</i> the incident response training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities.</p>		✓	✓
IR-2.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response training control is implemented.</p>		✓	✓
IR-2.5	<p><i>Interview</i> selected organizational personnel with incident response responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts incident response training on an ongoing basis.</p>			✓
IR-2.6	<p><i>Interview</i> selected organizational personnel with incident response responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident response training control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>IR-2 INCIDENT RESPONSE TRAINING <u>Control Enhancement:</u> (1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.</p>			✓
IR-2.7	<p><i>Examine</i> organizational records or documents to determine if incident response training events are simulated.</p>			✓
IR-2.8	<p><i>Interview</i> selected organizational personnel with incident response responsibilities to determine how simulated events improve the training process.</p>			✓

FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
IR-2.9	<i>Test selected simulated events to determine if organizational personnel respond as expected to the simulated crisis situation.</i>			✓
	IR-2 INCIDENT RESPONSE TRAINING <u>Control Enhancement:</u> (2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.			
IR-2.10	<i>Examine organizational records or documents to determine if the organization employs automated incident response training functions.</i>			
IR-2.11	<i>Interview selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the training process.</i>			
IR-2.12	<i>Test selected automated mechanisms to determine if the mechanisms are operating as intended.</i>			

FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>IR-3 INCIDENT RESPONSE TESTING <u>Control:</u> 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.</p>		✓	✓
IR-3.1	<p><i>Examine</i> organizational records or documents to determine if the organization tests its incident response capability using the organization-defined tests and exercises in accordance with the organization-defined frequency and documents the results of the tests.</p>		✓	✓
IR-3.2	<p><i>Examine</i> organizational records or documents to determine if the organization reviews incident response test results and takes corrective actions.</p>		✓	✓
IR-3.3	<p><i>Examine</i> organizational records or documents to determine if the incident response tests or exercises address key aspects of the incident response capability and if the tests or exercises confirm that the incident response objectives are met.</p>		✓	✓
IR-3.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response testing control is implemented.</p>		✓	✓
IR-3.5	<p><i>Interview</i> selected organizational personnel with incident response responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts incident response testing on an ongoing basis.</p>			✓
IR-3.6	<p><i>Interview</i> selected organizational personnel with incident response responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident response testing control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>IR-3 INCIDENT RESPONSE TESTING <u>Control Enhancement:</u> (1) The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.</p>			✓
IR-3.7	<p><i>Examine</i> organizational records or documents to determine what incident response testing functions are automated.</p>			✓
IR-3.8	<p><i>Interview</i> selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the testing process.</p>			✓
IR-3.9	<p><i>Test</i> selected automated mechanisms to determine if the mechanisms are operating as intended.</p>			✓

FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	IR-4 INCIDENT HANDLING <u>Control</u> : The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	✓	✓	✓
IR-4.1	<i>Examine</i> organizational records or documents to determine if the organization implements an incident handling capability for the information system that includes preparation, detection and analysis, containment, eradication, and recovery.	✓	✓	✓
IR-4.2	<i>Examine</i> organizational records or documents (or personnel engaged in incident handling activities) to determine if personnel are following designated incident handling procedures.		✓	✓
IR-4.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident handling control is implemented.		✓	✓
IR-4.4	<i>Interview</i> selected organizational personnel with incident response responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts incident handling for the information system on an ongoing basis.			✓
IR-4.5	<i>Interview</i> selected organizational personnel with incident response responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident handling control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	IR-4 INCIDENT HANDLING <u>Control Enhancement</u> : (1) The organization employs automated mechanisms to support the incident handling process.		✓	✓
IR-4.6	<i>Examine</i> organizational records or documents to determine if incident handling functions are automated.		✓	✓
IR-4.7	<i>Interview</i> selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the incident handling capability.			✓
IR-4.8	<i>Test</i> selected automated mechanisms to determine if the mechanisms are operating as intended.			✓

FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	IR-5 INCIDENT MONITORING <u>Control</u> : The organization tracks and documents information system security incidents on an ongoing basis.		✓	✓
IR-5.1	<i>Examine</i> organizational records or documents to determine if the organization tracks and documents information system security incidents on an ongoing basis.		✓	✓
IR-5.2	<i>Examine</i> organizational records or documents (or personnel engaged in incident monitoring activities) to determine if personnel are following designated incident monitoring procedures.		✓	✓
IR-5.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident monitoring control is implemented.		✓	✓
IR-5.4	<i>Interview</i> selected organizational personnel with incident response responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently tracks and documents information system incidents on an ongoing basis.			✓
IR-5.5	<i>Interview</i> selected organizational personnel with incident response responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident monitoring control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	IR-5 INCIDENT MONITORING <u>Control Enhancement</u> : (1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.			✓
IR-5.6	<i>Examine</i> organizational records or documents to determine if incident tracking and analysis functions are automated.			✓
IR-5.7	<i>Interview</i> selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the incident monitoring capability.			✓
IR-5.8	<i>Test</i> selected automated mechanisms to determine if the mechanisms are operating as intended.			✓

FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	IR-6 INCIDENT REPORTING <u>Control:</u> The organization promptly reports incident information to appropriate authorities.	✓	✓	✓
IR-6.1	<i>Examine</i> organizational records or documents to determine if the organization promptly reports incident information to appropriate authorities.	✓	✓	✓
IR-6.2	<i>Examine</i> organizational records or documents (or personnel engaged in incident reporting activities) to determine if personnel are following designated incident reporting procedures.		✓	✓
IR-6.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident reporting control is implemented.		✓	✓
IR-6.4	<i>Interview</i> selected organizational personnel with incident response responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently reports information system incidents on an ongoing basis.			✓
IR-6.5	<i>Interview</i> selected organizational personnel with incident response responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident reporting control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	IR-6 INCIDENT REPORTING <u>Control Enhancement:</u> (1) The organization employs automated mechanisms to assist in the reporting of security incidents.		✓	✓
IR-6.6	<i>Examine</i> organizational records or documents to determine if incident reporting functions are automated.		✓	✓
IR-6.7	<i>Interview</i> selected organizational personnel with incident response responsibilities to determine how the automated mechanisms improve the incident reporting capability.			✓
IR-6.8	<i>Test</i> selected automated mechanisms to determine if the mechanisms are operating as intended.			✓

FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>IR-7 INCIDENT RESPONSE ASSISTANCE <u>Control:</u> 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.</p>	✓	✓	✓
IR-7.1	<p><i>Examine</i> organizational records or documents 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.</p>	✓	✓	✓
IR-7.2	<p><i>Examine</i> organizational records or documents (or personnel engaged in incident response support activities) to determine if personnel are following designated incident response support procedures.</p>		✓	✓
IR-7.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the incident response assistance control is implemented.</p>		✓	✓
IR-7.4	<p><i>Interview</i> selected organizational personnel with incident response responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently provides incident response support on an ongoing basis.</p>			✓
IR-7.5	<p><i>Interview</i> selected organizational personnel with incident response responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the incident response assistance control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>IR-7 INCIDENT RESPONSE ASSISTANCE <u>Control Enhancement:</u> (1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.</p>		✓	✓
IR-7.6	<p><i>Examine</i> organizational records or documents to determine if incident response support functions are automated.</p>		✓	✓
IR-7.7	<p><i>Interview</i> selected organizational personnel with incident response support responsibilities to determine how the automated mechanisms improve the incident response support capability.</p>			✓
IR-7.8	<p><i>Test</i> selected automated mechanisms to determine if the mechanisms are operating as intended.</p>			✓

ASSESSMENT PROCEDURES

FAMILY: MAINTENANCE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES <u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	✓	✓	✓
MA-1.1	<i>Examine</i> organizational records or documents to determine if the information system maintenance 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.	✓	✓	✓
MA-1.2	<i>Examine</i> the information system maintenance policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	✓	✓	✓
MA-1.3	<i>Examine</i> the information system maintenance procedures to determine if the procedures are sufficient to address all areas identified in the information system maintenance policy and all associated information system maintenance controls.		✓	✓
MA-1.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system maintenance policy and procedures control is implemented.		✓	✓
MA-1.5	<i>Examine</i> the system maintenance policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance.			✓
MA-1.6	<i>Interview</i> selected organizational personnel with information system maintenance responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies the information system maintenance policy and procedures on an ongoing basis.			✓
MA-1.7	<i>Interview</i> selected organizational personnel with information system maintenance responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system maintenance policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: MAINTENANCE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>MA-2 PERIODIC MAINTENANCE <u>Control:</u> The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.</p>	✓	✓	✓
MA-2.1	<p><i>Examine</i> organizational records or documents to determine if the organization schedules and performs routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.</p>	✓	✓	✓
MA-2.2	<p><i>Examine</i> organizational records or documents to determine if the organization fully documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational periodic maintenance requirements.</p>	✓	✓	✓
MA-2.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the periodic maintenance control is implemented.</p>		✓	✓
MA-2.4	<p><i>Interview</i> selected organizational personnel with information system maintenance responsibilities and <i>examine</i> organizational records or documents to determine if the organization conducts periodic maintenance on an ongoing basis.</p>			✓
MA-2.5	<p><i>Interview</i> selected organizational personnel with information system maintenance responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the periodic maintenance control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>MA-2 PERIODIC MAINTENANCE <u>Control Enhancement:</u> (1) The organization maintains a maintenance log for the information system that includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).</p>		✓	✓
MA-2.6	<p><i>Examine</i> the maintenance log to determine if the log includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).</p>		✓	✓

FAMILY: MAINTENANCE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	MA-2 PERIODIC MAINTENANCE Control Enhancement: (2) The organization employs automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up-to date, accurate, complete, and available.			✓
MA-2.7	<i>Examine the automated mechanism(s) within the information system to determine if each automated function is properly configured to ensure that periodic maintenance is scheduled and conducted as required.</i>			✓
MA-2.8	<i>Examine the log of maintenance actions to determine if the log is up to date, accurate, complete, and available.</i>			✓

FAMILY: MAINTENANCE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	MA-3 MAINTENANCE TOOLS <u>Control:</u> The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.		✓	✓
MA-3.1	<i>Examine</i> organizational records or documents to determine if the organization approves, controls, and monitors information system maintenance tools.		✓	✓
MA-3.2	<i>Examine</i> approved information system maintenance tools and associated documentation to determine if the organization maintains the tools and documentation on an ongoing basis and if the processes applied are consistent with the documented maintenance procedures.		✓	✓
MA-3.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the maintenance tools control is implemented.		✓	✓
MA-3.4	<i>Interview</i> selected organizational personnel with information system maintenance responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently manages system maintenance tools on an ongoing basis.			✓
MA-3.5	<i>Interview</i> selected organizational personnel with information system maintenance responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the maintenance tools control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	MA-3 MAINTENANCE TOOLS <u>Control Enhancement:</u> (1) The organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.			✓
MA-3.6	<i>Interview</i> selected organizational personnel with information system maintenance responsibilities to determine if the organization inspects all maintenance tools used by maintenance personnel for improper modifications.			✓
MA-3.7	<i>Examine</i> organizational records or documents to determine if the organization inspects selected maintenance tools used by maintenance personnel to ensure that no improper modifications have been made.			✓

FAMILY: MAINTENANCE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>MA-3 MAINTENANCE TOOLS <u>Control Enhancement:</u> (2) The organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.</p>			✓
MA-3.8	<p><i>Interview selected organizational personnel with information system maintenance responsibilities to determine how the organization checks media containing diagnostic test programs for malicious code.</i></p>			✓
MA-3.9	<p><i>Examine organizational records or documents to determine if the organization checks for malicious code on all media containing diagnostic test programs before use within the information system.</i></p>			✓
	<p>MA-3 MAINTENANCE TOOLS <u>Control Enhancement:</u> (3) The organization checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.</p>			✓
MA-3.10	<p><i>Examine organizational records or documents to determine if the organization checks all maintenance equipment to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release.</i></p>			✓
MA-3.11	<p><i>Examine selected maintenance equipment that cannot be sanitized to ensure that the equipment is stored in a safe and secure location within the facility or is completely destroyed.</i></p>			✓
MA-3.12	<p><i>Examine organizational records or documents that indicate when maintenance equipment with organization information is removed from the facility that an organizational official explicitly authorizes the equipment removal.</i></p>			✓
	<p>MA-3 MAINTENANCE TOOLS <u>Control Enhancement:</u> (4) The organization employs automated mechanisms to ensure only authorized personnel use maintenance tools.</p>			
MA-3.13	<p><i>Examine organizational records or documents to determine if the organization uses automated mechanisms to control access to maintenance tools and if only authorized personnel have access to those tools.</i></p>			
MA-3.14	<p><i>Test the automated mechanism(s) within the information system to determine if each of the automated functions is properly configured to ensure that only authorized personnel access maintenance tools.</i></p>			

FAMILY: MAINTENANCE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	MA-4 REMOTE MAINTENANCE <u>Control:</u> The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.	✓	✓	✓
MA-4.1	<i>Examine</i> organizational records or documents to determine if the organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.	✓	✓	✓
MA-4.2	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the remote maintenance control is implemented.		✓	✓
MA-4.3	<i>Interview</i> selected organizational personnel with information system maintenance responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently approves, monitors, and controls remote maintenance on an ongoing basis.			✓
MA-4.4	<i>Interview</i> selected organizational personnel with information system maintenance responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the remote maintenance control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	MA-4 REMOTE MAINTENANCE <u>Control Enhancement:</u> (1) The organization audits all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions.			✓
MA-4.5	<i>Examine</i> organizational records or documents to determine if: (i) the organization audits all remote maintenance sessions and (ii) appropriate organizational personnel review the audit logs of the remote sessions.			✓
	MA-4 REMOTE MAINTENANCE <u>Control Enhancement:</u> (2) The organization addresses the installation and use of remote diagnostic links in the security plan for the information system.			✓
MA-4.6	<i>Examine</i> organizational records or documents to determine if the organization addresses the installation and use of remote diagnostic links for the information system.			✓

FAMILY: MAINTENANCE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>MA-4 REMOTE MAINTENANCE Control Enhancement: (3) Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced.</p>			✓
MA-4.7	<p><i>Examine the security level of the organization performing remote diagnostic or maintenance services to determine if the services performed are at an acceptable security level.</i></p>			✓

Draft

FAMILY: MAINTENANCE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>MA-5 MAINTENANCE PERSONNEL <u>Control:</u> The organization maintains a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.</p>	✓	✓	✓
MA-5.1	<p><i>Examine organizational records or documents to determine if: (i) the organization maintains a list of personnel authorized to perform maintenance on the information system; and (ii) only authorized personnel have performed maintenance on the information system.</i></p>	✓	✓	✓
MA-5.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the maintenance personnel control is implemented.</i></p>		✓	✓
MA-5.3	<p><i>Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if the organization consistently performs an authorization of maintenance personnel on an ongoing basis.</i></p>			✓
MA-5.4	<p><i>Interview selected organizational personnel with information system maintenance responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the maintenance personnel control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: MAINTENANCE

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>MA-6 TIMELY MAINTENANCE</p> <p><u>Control:</u> The organization obtains maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure.</p>		✓	✓
MA-6.1	<p><i>Examine</i> organizational records or documents to determine if maintenance support agreements and the inventory of spare parts are sufficient to support the organization-defined list of key information system components within the organization-defined time period of failure.</p>		✓	✓
MA-6.2	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the timely maintenance control is implemented.</p>		✓	✓
MA-6.3	<p><i>Interview</i> selected organizational personnel with information system maintenance responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently obtains timely maintenance for the information system on an ongoing basis.</p>			✓
MA-6.4	<p><i>Interview</i> selected organizational personnel with information system maintenance responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the timely maintenance control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

ASSESSMENT PROCEDURES

FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	MP-1 MEDIA PROTECTION POLICY AND PROCEDURES <u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	✓	✓	✓
MP-1.1	<i>Examine organizational records or documents to determine if the media protection 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 reviews indicate updates are required.</i>	✓	✓	✓
MP-1.2	<i>Examine the media protection policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</i>	✓	✓	✓
MP-1.3	<i>Examine the media protection procedures to determine if the procedures are sufficient to address all areas identified in the media protection policy and all associated media protection controls.</i>		✓	✓
MP-1.4	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media protection policy and procedures control is implemented.</i>		✓	✓
MP-1.5	<i>Examine the media protection policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance.</i>			✓
MP-1.6	<i>Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently applies the media protection policy and procedures on an ongoing basis.</i>			✓
MP-1.7	<i>Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media protection policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓

FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>MP-2 MEDIA ACCESS <u>Control:</u> The organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.</p>	✓	✓	✓
MP-2.1	<p><i>Examine</i> organizational records or documents and/or physical facilities containing media devices to determine if only authorized users have access to information in printed form or on digital media removed from the information system.</p>	✓	✓	✓
MP-2.2	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media access control is implemented.</p>		✓	✓
MP-2.3	<p><i>Interview</i> selected organizational personnel with media protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently restricts media access on an ongoing basis.</p>			✓
MP-2.4	<p><i>Interview</i> selected organizational personnel with media protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media access control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>MP-2 MEDIA ACCESS <u>Control Enhancement:</u> (1) Unless guard stations control access to media storage areas, the organization employs automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted.</p>			✓
MP-2.5	<p><i>Examine</i> media storage areas to determine if guard stations control access to media or if automated mechanisms are implemented to control access to media.</p>			✓
MP-2.6	<p><i>Examine</i> organizational records or documents to determine if: (i) the organization employs automated mechanisms to ensure only authorized access to media storage areas and to audit access attempts and access granted; and (ii) the types of automated mechanisms and automated functions are configured to ensure only authorized access to such storage areas and to audit access attempts and access granted.</p>			✓
MP-2.7	<p><i>Test</i> the automated mechanism(s) within the information system to determine if each automated function is properly configured to ensure that media access is restricted as required.</p>			✓

FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>MP-3 MEDIA LABELING</p> <p><u>Control:</u> The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information. The organization exempts the following specific types of media or hardware components from labeling so long as they remain within a secure environment: [Assignment: organization-defined list of media types and hardware components].</p>		✓	✓
MP-3.1	<p><i>Examine</i> organizational records or documents to determine if the organization: (i) affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information; and (ii) exempts specific types of media or hardware components from labeling so long as they remain within a secure environment.</p>		✓	✓
MP-3.2	<p><i>Examine</i> a sample of media, both storage media and system output, to determine if the media are affixed with labels indicating the distribution limitations and handling caveats of the information.</p>		✓	✓
MP-3.3	<p><i>Examine</i> the organization-defined list of media types and hardware components that specifies types of media or hardware components that are exempt from labeling so long as they remain within a secure environment.</p>		✓	✓
MP-3.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media labeling control is implemented.</p>		✓	✓
MP-3.5	<p><i>Interview</i> selected organizational personnel with media protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies media labeling on an ongoing basis.</p>			✓
MP-3.6	<p><i>Interview</i> selected organizational personnel with media protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media labeling control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>MP-4 MEDIA STORAGE</p> <p><u>Control:</u> The organization physically controls and securely stores information system media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media.</p>		✓	✓
MP-4.1	<p><i>Examine organizational records or documents to determine if the organization protects information system media at the highest FIPS 199 security category for the information system until the media is destroyed or sanitized using approved equipment, techniques, and procedures.</i></p>		✓	✓
MP-4.2	<p><i>Examine the location where the organization physically controls and securely stores information system media, both paper and digital, to determine if the organization controls the media at the highest FIPS 199 security category of the information recorded on the media.</i></p>		✓	✓
MP-4.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media storage control is implemented.</i></p>		✓	✓
MP-4.4	<p><i>Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if the organization consistently controls and securely stores information system media on an ongoing basis.</i></p>			✓
MP-4.5	<p><i>Interview selected organizational personnel with media protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media storage control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>MP-5 MEDIA TRANSPORT <u>Control:</u> The organization controls information system media (paper and digital) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.</p>		✓	✓
MP-5.1	<p><i>Examine</i> organizational records or documents to determine if the organization restricts the pickup, receipt, transfer, and delivery of information system media (paper and digital) to authorized personnel.</p>		✓	✓
MP-5.2	<p><i>Examine</i> the list of personnel that have been authorized for the pickup, receipt, transfer, and delivery of information system media to determine if access is appropriately restricted.</p>		✓	✓
MP-5.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media transport control is implemented.</p>		✓	✓
MP-5.4	<p><i>Interview</i> selected organizational personnel with media protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently transports in a secure manner information system media on an ongoing basis.</p>			✓
MP-5.5	<p><i>Interview</i> selected organizational personnel with media protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media transport control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>MP-6 MEDIA SANITIZATION AND DISPOSAL</p> <p><u>Control:</u> The organization: (i) sanitizes information system media, both paper and digital, prior to disposal or release for reuse; (ii) tracks, documents, and verifies media sanitization actions; and (iii) periodically tests sanitization equipment and procedures to ensure correct performance.</p>	✓	✓	✓
MP-6.1	<p><i>Examine</i> organizational records or documents to determine if the organization: (i) sanitizes information system media, both paper and digital, using approved equipment, techniques, and procedures prior to disposal or release for reuse; (ii) tracks, documents, and verifies media sanitization actions; and (iii) conducts periodic tests of sanitization equipment to ensure correct performance.</p>	✓	✓	✓
MP-6.2	<p><i>Examine</i> organizational records or documents to determine if the organization sanitizes information system media, both paper and digital, using approved equipment, techniques, and procedures prior to disposal or release for reuse consistent with NIST Special Publication 800-88.</p>	✓	✓	✓
MP-6.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the media sanitization and disposal control is implemented.</p>		✓	✓
MP-6.4	<p><i>Interview</i> selected organizational personnel with media protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies media sanitization and disposal on an ongoing basis.</p>			✓
MP-6.5	<p><i>Interview</i> selected organizational personnel with media protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the media sanitization and disposal control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

ASSESSMENT PROCEDURES

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES</p> <p><u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.</p>	✓	✓	✓
PE-1.1	<p><i>Examine organizational records or documents to determine if the physical and environmental protection 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.</i></p>	✓	✓	✓
PE-1.2	<p><i>Examine the physical and environmental protection policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</i></p>	✓	✓	✓
PE-1.3	<p><i>Examine the physical and environmental protection procedures to determine if the procedures are sufficient to address all areas identified in the physical and environmental protection policy and all associated physical and environmental protection controls.</i></p>		✓	✓
PE-1.4	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical and environmental protection policy and procedures control is implemented.</i></p>		✓	✓
PE-1.5	<p><i>Examine the physical and environmental protection policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance.</i></p>			✓
PE-1.6	<p><i>Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently applies the physical and environmental protection policy and procedures on an ongoing basis.</i></p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
PE-1.7	<i>Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the physical and environmental protection policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓

Draft

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-2 PHYSICAL ACCESS AUTHORIZATIONS</p> <p><u>Control:</u> The organization develops and keeps current lists of personnel with authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials [<i>Assignment: organization-defined frequency, at least annually</i>].</p>	✓	✓	✓
PE-2.1	<p><i>Examine</i> organizational records or documents to determine if: (i) the organization develops and keeps current a list of personnel with authorized access to the facility containing the information system; (ii) the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards); and (iii) designated officials within the organization review and approve the access list and authorization credentials on an organization-defined frequency.</p>	✓	✓	✓
PE-2.2	<p><i>Examine</i> the facility access list to determine if: (i) the individuals on the list are current personnel assigned to the organization; and (ii) the authorization credentials of the personnel are appropriate.</p>		✓	✓
PE-2.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access authorizations control is implemented.</p>		✓	✓
PE-2.4	<p><i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization manages physical access authorizations for the facility on an ongoing basis.</p>			✓
PE-2.5	<p><i>Interview</i> selected organizational personnel with physical and environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the physical access authorizations control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-3 PHYSICAL ACCESS CONTROL</p> <p><u>Control:</u> The organization controls all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities. The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization’s assessment of risk.</p>	✓	✓	✓
PE-3.1	<p><i>Examine</i> organizational records or documents and the facility that contains the information system to determine if the organization: (i) controls all physical access points to the facility; (ii) verifies individual access authorizations before granting access to the facility; and (iii) controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization’s assessment of risk.</p>	✓	✓	✓
PE-3.2	<p><i>Examine</i> organizational records or documents and selected physical access devices to determine if: (i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis; (ii) the organization secures keys, combinations and other access devices on a regular basis; and (iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated.</p>		✓	✓
PE-3.3	<p><i>Examine</i> organizational records or documents and selected physical access devices to determine if: (i) the access control system conforms to the requirements of FIPS 201 and NIST Special Publication 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed); (ii) the access control system conforms to the requirements of NIST Special Publication 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system conforms to the requirements of NIST Special Publication 800-76 (where the token-based access control function employs biometric verification).</p>		✓	✓
PE-3.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the physical access control is implemented.</p>		✓	✓
PE-3.5	<p><i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently controls physical access to the facility where the information system resides on an ongoing basis.</p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
PE-3.6	<i>Interview</i> selected organizational personnel with physical and environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the physical access control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

Draft

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM</p> <p><u>Control:</u> The organization controls physical access to information system distribution and transmission lines within organizational facilities to prevent accidental damage, eavesdropping, in-transit modification, disruption, or physical tampering.</p>			✓
PE-4.1	<p><i>Examine organizational records or documents and the facility where the information system resides to determine if the organization controls physical access to information system distribution and transmission lines to prevent accidental damage, eavesdropping, in-transit modification, disruption, or physical tampering.</i></p>			✓
PE-4.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control for transmission medium control is implemented.</i></p>			✓
PE-4.3	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization consistently controls physical access to system distribution and transmission lines on an ongoing basis.</i></p>			✓
PE-4.4	<p><i>Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access control for transmission medium control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-5 ACCESS CONTROL FOR DISPLAY MEDIUM <u>Control:</u> The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.</p>		✓	✓
PE-5.1	<p><i>Examine organizational records, documents, and the facility where the information system resides to determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.</i></p>		✓	✓
PE-5.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access control for display medium control is implemented.</i></p>		✓	✓
PE-5.3	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization consistently controls physical access to system devices that display information on an ongoing basis.</i></p>			✓
PE-5.4	<p><i>Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access control for display medium control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	PE-6 MONITORING PHYSICAL ACCESS <u>Control:</u> The organization monitors physical access to information systems to detect and respond to incidents.	✓	✓	✓
PE-6.1	<i>Examine</i> organizational records, documents, and the facility where the information system resides to determine if the organization monitors physical access to information systems to detect and respond to incidents.	✓	✓	✓
PE-6.2	<i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities to determine how individuals respond to physical access incidents.		✓	✓
PE-6.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the monitoring physical access control is implemented.		✓	✓
PE-6.4	<i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records, documents, and the facility where the information system resides to determine if the organization consistently monitors physical access to the system to detect and respond to incidents on an ongoing basis.			✓
PE-6.5	<i>Interview</i> selected organizational personnel with physical and environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the monitoring physical access control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	PE-6 MONITORING PHYSICAL ACCESS <u>Control Enhancement:</u> (1) The organization monitors real-time intrusion alarms and surveillance equipment.		✓	✓
PE-6.6	<i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities to determine if real-time intrusion alarms and surveillance equipment are used.		✓	✓
PE-6.7	<i>Examine</i> intrusion alarms and surveillance equipment to determine if the equipment is operational and functioning properly.		✓	✓
	PE-6 MONITORING PHYSICAL ACCESS <u>Control Enhancement:</u> (2) The organization employs automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.			✓

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

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
PE-6.8	<i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities to determine if the organization employs automated mechanisms to recognize potential intrusions and initiate appropriate responses.			✓
PE-6.9	<i>Examine</i> organizational documents or records to determine if physical access intrusions are recognized and appropriate actions initiated.			✓
PE-6.10	<i>Test</i> the automated mechanisms to determine if each automated function is properly configured to recognize potential intrusions and initiate appropriate responses.			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-7 VISITOR CONTROL <u>Control:</u> The organization controls physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.</p>	✓	✓	✓
PE-7.1	<p><i>Examine organizational records, documents, and the facility where the information system resides to determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility or areas other than areas designated as publicly accessible.</i></p>	✓	✓	✓
PE-7.2	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities to determine if the Personal Identity Verification (PIV) credentials for federal government employees and contractors conform to FIPS 201, and the issuing organizations for the PIV credentials are accredited in accordance with the provisions of NIST Special Publication 800-79.</i></p>		✓	✓
PE-7.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the visitor control is implemented.</i></p>		✓	✓
PE-7.4	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization controls visitor access to the facility on an ongoing basis.</i></p>			✓
PE-7.5	<p><i>Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the visitor control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓
	<p>PE-7 VISITOR CONTROL <u>Control Enhancement:</u> (1) The organization escorts visitors and monitors visitor activity, when required.</p>		✓	✓
PE-7.6	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization escorts visitors and monitors visitor activity, when required.</i></p>		✓	✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-8 ACCESS LOGS</p> <p><u>Control:</u> The organization maintains a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the access logs [<i>Assignment: organization-defined frequency</i>].</p>	✓	✓	✓
PE-8.1	<p><i>Examine</i> organizational records or documents to determine if the organization maintains a visitor access log to the facility where the information system resides that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; (vii) name and organization of person visited; and (viii) an indication of a designated official's review of the access log within the organization-defined frequency.</p>	✓	✓	✓
PE-8.2	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access logs control is implemented.</p>		✓	✓
PE-8.3	<p><i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently maintains and reviews visitor access logs on an ongoing basis.</p>			✓
PE-8.4	<p><i>Interview</i> selected organizational personnel with physical and environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access logs control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>PE-8 ACCESS LOGS</p> <p><u>Control Enhancement:</u></p> <p>(1) The organization employs automated mechanisms to facilitate the maintenance and review of access logs.</p>			✓
PE-8.5	<p><i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities to determine what automated mechanisms and automated functions are employed to facilitate the maintenance and review of visitor access logs.</p>			✓
PE-8.6	<p><i>Examine</i> the automated mechanisms within the facility to determine if each automated function is properly configured to ensure that maintenance and review of visitor access logs are properly performed.</p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-9 POWER EQUIPMENT AND POWER CABLING <u>Control:</u> The organization protects power equipment and power cabling for the information system from damage and destruction.</p>		✓	✓
PE-9.1	<p><i>Examine</i> organizational records, documents, and the facility where the information system resides to determine if the organization protects power equipment and power cabling for the information system from damage and destruction.</p>		✓	✓
PE-9.2	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the power equipment and power cabling control is implemented.</p>		✓	✓
PE-9.3	<p><i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently protects power equipment and power cabling for the information system on an ongoing basis.</p>			✓
PE-9.4	<p><i>Interview</i> selected organizational personnel with physical and environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the power equipment and power cabling control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>PE-9 POWER EQUIPMENT AND POWER CABLING <u>Control Enhancement:</u> (1) The organization employs redundant and parallel power cabling paths.</p>			
PE-9.5	<p><i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records, documents, and the facility where the information system resides to determine if the organization employs redundant and parallel power cabling paths.</p>			

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-10 EMERGENCY SHUTOFF</p> <p><u>Control:</u> For specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms), the organization provides the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.</p>		✓	✓
PE-10.1	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility containing concentrations of information system resources to determine if the organization provides the capability of shutting off power to any information system component that may be malfunctioning or threatened.</i></p>		✓	✓
PE-10.2	<p><i>Examine the emergency shutoff capability to ensure that it exists and is functional.</i></p>		✓	✓
PE-10.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the emergency shutoff control is implemented.</i></p>		✓	✓
PE-10.4	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility containing concentrations of information system resources to determine if the organization consistently employs an emergency shutoff capability for the information system on an ongoing basis.</i></p>			✓
PE-10.5	<p><i>Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the emergency shutoff control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-11 EMERGENCY POWER <u>Control:</u> The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.</p>		✓	✓
PE-11.1	<p><i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records, documents, and the facility where the information system resides to determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the system in the event of a primary power source loss.</p>		✓	✓
PE-11.2	<p><i>Examine</i> organizational records or documents to determine if the results of the last tested power outage demonstrated the availability of a short-term power supply for the information system.</p>		✓	✓
PE-11.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the emergency power control is implemented.</p>		✓	✓
PE-11.4	<p><i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records, documents, and the facility where the information system resides to determine if the organization consistently provides an emergency power capability for the information system on an ongoing basis.</p>			✓
PE-11.5	<p><i>Interview</i> selected organizational personnel with physical and environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the emergency power control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>PE-11 EMERGENCY POWER <u>Control Enhancement:</u> (1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.</p>			✓
PE-11.6	<p><i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.</p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
PE-11.7	<i>Examine</i> organizational records or documents to determine if the results of the last tested power outage demonstrated the availability of a long-term alternate power supply for the information system.			✓
	<p>PE-11 EMERGENCY POWER <u>Control Enhancement:</u> (2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.</p>			
PE-11.8	<i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.			
PE-11.9	<i>Examine</i> organizational records or documents to determine if the results of the last tested power outage demonstrated the availability of a long-term, self-contained alternate power supply for the information system.			

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-12 EMERGENCY LIGHTING <u>Control:</u> The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.</p>	✓	✓	✓
PE-12.1	<p><i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records, documents, and the facility where the information system resides to determine if the organization employs and maintains an automatic emergency lighting system that activate in the event of a power outage or disruption and that covers emergency exits and evacuation routes.</p>	✓	✓	✓
PE-12.2	<p><i>Examine</i> organizational records or documents to determine if the results of the last tested power outage demonstrated that the emergency lighting system was operational and fully functional.</p>		✓	✓
PE-12.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the emergency lighting control is implemented.</p>		✓	✓
PE-12.4	<p><i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization provides and maintains an emergency lighting system for the information system on an ongoing basis.</p>			✓
PE-12.5	<p><i>Interview</i> selected organizational personnel with physical and environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the emergency lighting control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	PE-13 FIRE PROTECTION <u>Control:</u> The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.	✓	✓	✓
PE-13.1	<i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records, documents, and the facility where the information system resides to determine if the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.	✓	✓	✓
PE-13.2	<i>Examine</i> the results of the last test of the fire suppression and detection devices/systems to determine if the fire protection resources can be successfully activated in the event of a fire.		✓	✓
PE-13.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the fire protection control is implemented.		✓	✓
PE-13.4	<i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently provides fire suppression and detection devices/systems for the facility where the information system resides on an ongoing basis.			✓
PE-13.5	<i>Interview</i> selected organizational personnel with physical and environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the fire protection control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	PE-13 FIRE PROTECTION <u>Control Enhancement:</u> (1) Fire suppression and detection devices/systems activate automatically in the event of a fire.		✓	✓
PE-13.6	<i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if fire suppression and detection devices/systems activate automatically in the event of a fire.		✓	✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-13 FIRE PROTECTION Control Enhancement: (2) Fire suppression and detection devices/systems provide automatic notification of any activation to the organization and emergency responders.</p>			✓
PE-13.7	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities to determine if the fire suppression and detection devices/systems for the facility where the information system resides provide automatic notification of any activation to the organization and emergency responders.</i></p>			✓
PE-13.8	<p><i>Examine the alarm system service level agreement to determine if the agreement details automatic notification to the organization and emergency responders.</i></p>			✓
PE-13.9	<p><i>Examine organizational records or documents to determine if the results of the last test of the fire suppression and detection devices/systems demonstrated that the organization and emergency responders were automatically notified.</i></p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-14 TEMPERATURE AND HUMIDITY CONTROLS</p> <p><u>Control:</u> The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within facilities containing information systems.</p>	✓	✓	✓
PE-14.1	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization regularly maintains, within acceptable levels, and monitors the temperature and humidity of the facility where the information system resides.</i></p>	✓	✓	✓
PE-14.2	<p><i>Examine the facility where the information system resides to determine if the temperature and humidity controlling systems are in place and functioning as intended.</i></p>	✓	✓	✓
PE-14.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the temperature and humidity control is implemented.</i></p>		✓	✓
PE-14.4	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently maintains and monitors temperature and humidity levels within the facility where the information system resides on an ongoing basis.</i></p>			✓
PE-14.5	<p><i>Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the temperature and humidity control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-15 WATER DAMAGE PROTECTION <u>Control:</u> The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.</p>	✓	✓	✓
PE-15.1	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization protects the information system from water damage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.</i></p>	✓	✓	✓
PE-15.2	<p><i>Examine the facility where the information system resides to determine if the master shutoff valves are accessible and working properly.</i></p>	✓	✓	✓
PE-15.3	<p><i>Examine organizational records or documents to determine if the results of the last test of the environmental controls of the facility where the information system resides demonstrate that the master shutoff valves are working properly.</i></p>		✓	✓
PE-15.4	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the water damage protection control is implemented.</i></p>		✓	✓
PE-15.5	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently protects the information system from water damage on an ongoing basis.</i></p>			✓
PE-15.6	<p><i>Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the water damage protection control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓
	<p>PE-15 WATER DAMAGE PROTECTION <u>Control Enhancement:</u> (1) The organization employs automated mechanisms to automatically close shutoff valves in the event of a significant water leak.</p>			✓
PE-15.7	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities to determine if automated mechanisms and automated functions are employed to automatically close shutoff valves in the event of a significant water leak.</i></p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
PE-15.8	<i>Examine the automated mechanisms for water shutoff valves within the facility to determine if each automated function is properly configured to ensure that water valves can be automatically shut off in the event of a significant water leak.</i>			✓

Draft

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-16 DELIVERY AND REMOVAL <u>Control:</u> The organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.</p>	✓	✓	✓
PE-16.1	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization controls the information system-related items (i.e., hardware, firmware, software) entering and exiting the facility where the system resides and maintains appropriate records of those items.</i></p>	✓	✓	✓
PE-16.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the delivery and removal control is implemented.</i></p>		✓	✓
PE-16.3	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization consistently controls the delivery and removal of information system-related items from the facility where the system resides on an ongoing basis.</i></p>			✓
PE-16.4	<p><i>Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the delivery and removal control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

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

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	PE-17 ALTERNATE WORK SITE <u>Control:</u> Individuals within the organization employ appropriate information system security controls at alternate work sites.		✓	✓
PE-17.1	<i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if individuals within the organization employ appropriate information system security controls at alternate work sites.</i>		✓	✓
PE-17.2	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the alternate work site control is implemented.</i>		✓	✓
PE-17.3	<i>Examine the alternate work sites to determine if appropriate information system security controls are in place.</i>			✓
PE-17.4	<i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and alternate work sites to determine if individuals within the organization consistently employ appropriate information system security controls at alternate work sites on an ongoing basis.</i>			✓
PE-17.5	<i>Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the alternate work site control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS <u>Control:</u> The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.</p>		✓	✓
PE-18.1	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records or documents to determine if the organization positions information system components within the facility to minimize potential damage from environmental hazards (e.g., electrical interference, electromagnetic radiation, vandalism, eating, drinking, smoking in the proximity, information leakage due to emanation) and to minimize the opportunity for unauthorized access.</i></p>		✓	✓
PE-18.2	<p><i>Examine the facility where the information system components reside to determine if the organization positions components to minimize potential damage from environmental hazards and to minimize the opportunity for unauthorized access.</i></p>		✓	✓
PE-18.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the location of information system components control is implemented.</i></p>		✓	✓
PE-18.4	<p><i>Interview selected organizational personnel with physical and/or environmental protection responsibilities and examine organizational records, documents, and the facility where the information system resides to determine if the organization consistently manages the location of system components to minimize risk on an ongoing basis.</i></p>			✓
PE-18.5	<p><i>Interview selected organizational personnel with physical and environmental protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the location of information system components control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PE-19 INFORMATION LEAKAGE <u>Control:</u> The organization protects the information system from information leakage due to electromagnetic signals emanations.</p>			
PE-19.1	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information leakage control is implemented.</p>			
PE-19.2	<p><i>Interview</i> selected organizational personnel with physical and/or environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently protects the information system from information leakage due to electromagnetic signals emanations on an ongoing basis.</p>			
PE-19.3	<p><i>Interview</i> selected organizational personnel with physical and environmental protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information leakage control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			

ASSESSMENT PROCEDURES

FAMILY: PLANNING

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PL-1 SECURITY PLANNING POLICY AND PROCEDURES</p> <p><u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.</p>	✓	✓	✓
PL-1.1	<p><i>Examine</i> organizational records or documents to determine if security 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.</p>	✓	✓	✓
PL-1.2	<p><i>Examine</i> the security planning policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</p>	✓	✓	✓
PL-1.3	<p><i>Examine</i> the security planning procedures to determine if the procedures are sufficient to address all areas identified in the security planning policy and all associated security planning controls.</p>		✓	✓
PL-1.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security planning policy and procedures control is implemented.</p>		✓	✓
PL-1.5	<p><i>Examine</i> the security planning policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance.</p>			✓
PL-1.6	<p><i>Interview</i> selected organizational personnel with security planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies the security planning policy and procedures on an ongoing basis.</p>			✓
PL-1.7	<p><i>Interview</i> selected organizational personnel with security planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security planning policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: PLANNING

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PL-2 SYSTEM SECURITY PLAN</p> <p><u>Control:</u> The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.</p>	✓	✓	✓
PL-2.1	<p><i>Examine organizational records or documents to determine if the security plan: (i) exists; (ii) is documented; (iii) is disseminated to appropriate elements within the organization; and (iv) is reviewed and approved by responsible officials within the organization.</i></p>	✓	✓	✓
PL-2.2	<p><i>Examine the security plan to determine if the plan is consistent with NIST Special Publication 800-18 and addresses security roles, responsibilities, assigned individuals with contact information, and activities for planning security of the information system.</i></p>	✓	✓	✓
PL-2.3	<p><i>Interview selected organizational personnel with security planning and plan implementation responsibilities to determine if key operating elements within the organization understand the security plan and are ready to implement the plan.</i></p>		✓	✓
PL-2.4	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system security plan control is implemented.</i></p>		✓	✓
PL-2.5	<p><i>Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if organizational officials consistently review and approve the security plan for the information system on an ongoing basis.</i></p>			✓
PL-2.6	<p><i>Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system security plan control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: PLANNING

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PL-3 SYSTEM SECURITY PLAN UPDATE <u>Control:</u> The organization reviews the security plan for the information system [Assignment: organization-defined frequency] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.</p>	✓	✓	✓
PL-3.1	<i>Examine</i> organizational records or documents to determine if the security plan is updated in accordance with organization-defined frequency.	✓	✓	✓
PL-3.2	<i>Examine</i> the security plan to determine if the revised plan reflects the needed changes based on the organization’s experiences during plan implementation.		✓	✓
PL-3.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system security plan update control is implemented.		✓	✓
PL-3.4	<i>Interview</i> selected organizational personnel with security planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently reviews and updates the security plan for the information system on an ongoing basis.			✓
PL-3.5	<i>Interview</i> selected organizational personnel with security planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security plan update control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: PLANNING

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PL-4 RULES OF BEHAVIOR</p> <p><u>Control:</u> The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.</p>	✓	✓	✓
PL-4.1	<p><i>Examine</i> organizational records or documents to determine if the organization provides and makes readily available to all information system users a set of rules that describes users responsibilities and expected behavior with regard to information and information system usage.</p>	✓	✓	✓
PL-4.2	<p><i>Examine</i> organizational records or documents to determine if the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.</p>	✓	✓	✓
PL-4.3	<p><i>Examine</i> the rules of behavior to determine if the content is consistent with NIST Special Publication 800-18.</p>	✓	✓	✓
PL-4.4	<p><i>Interview</i> selected organizational personnel to determine if they understand the rules of behavior for the information system.</p>		✓	✓
PL-4.5	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the rules of behavior control is implemented.</p>		✓	✓
PL-4.6	<p><i>Interview</i> selected organizational personnel with security planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently reviews and updates the rules of behavior on an ongoing basis.</p>			✓
PL-4.7	<p><i>Interview</i> selected organizational personnel with security planning and plan implementation responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the rules of behavior control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: PLANNING

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PL-5 PRIVACY IMPACT ASSESSMENT <u>Control:</u> The organization conducts a privacy impact assessment on the information system.</p>	✓	✓	✓
PL-5.1	<p><i>Examine organizational records or documents to determine if the organization conducts a privacy impact assessment on the information system.</i></p>	✓	✓	✓
PL-5.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the privacy impact assessment control is implemented.</i></p>		✓	✓
PL-5.3	<p><i>Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently conducts privacy impact assessments on the information system on an ongoing basis.</i></p>			✓
PL-5.4	<p><i>Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the privacy impact assessment control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: PLANNING

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PL-6 SECURITY-RELATED ACTIVITY PLANNING</p> <p><u>Control:</u> The organization ensures that appropriate planning and coordination occur before conducting security-related activities affecting the information system in order to minimize the impact on organizational operations (i.e., mission, functions, image, and reputation) and organizational assets.</p>		✓	✓
PL-6.1	<p><i>Examine organizational records or documents to determine if appropriate planning and coordination occur before conducting security-related activities affecting the information system.</i></p>		✓	✓
PL-6.2	<p><i>Interview selected organizational personnel with security planning and plan implementation responsibilities to determine if key operating elements within the organization understand the breath and depth of ongoing security-related activities in order to minimize the impact on organizational operations (i.e., mission, functions, image, and reputation) and organizational assets.</i></p>		✓	✓
PL-6.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security-related activity planning control is implemented.</i></p>		✓	✓
PL-6.4	<p><i>Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if the organization consistently plans and coordinates with appropriate organizational elements prior to initiating security-related activities on an ongoing basis.</i></p>			✓
PL-6.5	<p><i>Interview selected organizational personnel with security planning and plan implementation responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security-related activity planning control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

ASSESSMENT PROCEDURES

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES <u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	✓	✓	✓
PS-1.1	<i>Examine organizational records or documents to determine if the personnel security 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.</i>	✓	✓	✓
PS-1.2	<i>Examine the personnel security policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</i>	✓	✓	✓
PS-1.3	<i>Examine the personnel security procedures to determine if the procedures are sufficient to address all areas identified in the personnel security policy and all associated personnel security controls.</i>		✓	✓
PS-1.4	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel security policy and procedures control is implemented.</i>		✓	✓
PS-1.5	<i>Examine the personnel security policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance.</i>			✓
PS-1.6	<i>Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if the organization consistently applies the personnel security policy and procedures on an ongoing basis.</i>			✓
PS-1.7	<i>Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel security policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PS-2 POSITION CATEGORIZATION</p> <p><u>Control</u>: The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [<i>Assignment: organization-defined frequency</i>].</p>	✓	✓	✓
PS-2.1	<p><i>Examine</i> the organizational records or documents to determine if the organization: (i) establishes risk designations; (ii) assigns a risk designation to all organizational positions; (iii) follows screening criteria for individuals filling organizational positions; and (iv) reviews and revises position risk designations on an organization-defined frequency.</p>	✓	✓	✓
PS-2.2	<p><i>Test</i> the position categorization procedures by comparing a list of organizational personnel and their clearance and/or authorization levels to the position risk designations to determine if the organization meets the screening criteria for those individuals filling the positions.</p>		✓	✓
PS-2.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the position categorization control is implemented.</p>		✓	✓
PS-2.4	<p><i>Interview</i> selected organizational personnel with personnel security responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently assigns risk designations for positions within the organization and establishes screening criteria for those positions on an ongoing basis.</p>			✓
PS-2.5	<p><i>Interview</i> selected organizational personnel with personnel security responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the position categorization control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PS-3 PERSONNEL SCREENING</p> <p><u>Control:</u> The organization screens individuals requiring access to organizational information and information systems before authorizing access.</p>	✓	✓	✓
PS-3.1	<p><i>Examine organizational records or documents to determine if the organization appropriately screens individuals requiring access to organizational information and information systems prior to authorizing access.</i></p>	✓	✓	✓
PS-3.2	<p><i>Test the personnel screening process by comparing a list of organizational personnel requiring access to the information system and their associated screening dates to account creation dates to determine if the organization meets the screening criteria for those individuals.</i></p>		✓	✓
PS-3.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel screening control is implemented.</i></p>		✓	✓
PS-3.4	<p><i>Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if the organization consistently conducts personnel screening for positions within the organization on an ongoing basis.</i></p>			✓
PS-3.5	<p><i>Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel screening control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PS-4 PERSONNEL TERMINATION</p> <p><u>Control:</u> When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.</p>	✓	✓	✓
PS-4.1	<p><i>Examine organizational records or documents to determine if the organization: (i) revokes the information system accounts of terminated personnel; (ii) conducts exit interviews of terminated personnel; (iii) collects all information system-related property (e.g., keys, identification cards, building passes) of terminated personnel; and (iv) retains access to official documents and records on organizational information systems created by terminated personnel.</i></p>	✓	✓	✓
PS-4.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel termination control is implemented.</i></p>		✓	✓
PS-4.3	<p><i>Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if the organization consistently manages personnel termination activities to protect organizational operations and assets on an ongoing basis.</i></p>			✓
PS-4.4	<p><i>Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel termination control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PS-5 PERSONNEL TRANSFER</p> <p><u>Control:</u> The organization reviews information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).</p>	✓	✓	✓
PS-5.1	<p><i>Examine organizational records or documents to determine if the organization: (i) reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and (ii) initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization.</i></p>	✓	✓	✓
PS-5.2	<p><i>Test the personnel transfer procedures of the organization by comparing the information system authorizations of current personnel to the access authorizations of transferred personnel to determine if all personnel have appropriate authorizations for the information system.</i></p>		✓	✓
PS-5.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel transfer control is implemented.</i></p>		✓	✓
PS-5.4	<p><i>Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if the organization consistently manages personnel transfer activities to protect organizational operations and assets on an ongoing basis.</i></p>			✓
PS-5.5	<p><i>Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel transfer control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PS-6 ACCESS AGREEMENTS</p> <p><u>Control:</u> The organization completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [Assignment: organization-defined frequency].</p>	✓	✓	✓
PS-6.1	<p><i>Examine</i> organizational records or documents to determine if the organization: (i) completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access; and (ii) reviews and updates the access agreements on an organization-defined frequency.</p>	✓	✓	✓
PS-6.2	<p><i>Examine</i> selected access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for the information system to determine if the access agreements are: (i) signed and retained in accordance with the documented organizational policy and procedures; and (ii) reviewed and updated by the organization on an organization-defined frequency.</p>		✓	✓
PS-6.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the access agreements control is implemented.</p>		✓	✓
PS-6.4	<p><i>Interview</i> selected organizational personnel with personnel security responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently completes, reviews, and updates access agreements on an ongoing basis.</p>			✓
PS-6.5	<p><i>Interview</i> selected organizational personnel with personnel security responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the access agreements control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PS-7 THIRD-PARTY PERSONNEL SECURITY</p> <p><u>Control:</u> The organization establishes personnel security requirements including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitors provider compliance to ensure adequate security.</p>	✓	✓	✓
PS-7.1	<p><i>Examine organizational records or documents to determine if the organization:(i) establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management); and (ii) monitors third-party provider compliance to ensure adequate security.</i></p>	✓	✓	✓
PS-7.2	<p><i>Examine organizational records or documents to determine if the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST Special Publication 800-35.</i></p>		✓	✓
PS-7.3	<p><i>Interview selected organizational personnel with personnel security responsibilities to determine if the organization monitors third-party provider compliance with personnel security requirements.</i></p>		✓	✓
PS-7.4	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the third-party personnel security control is implemented.</i></p>		✓	✓
PS-7.5	<p><i>Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if the organization consistently establishes and monitors personnel security requirements for third-party providers on an ongoing basis.</i></p>			✓
PS-7.6	<p><i>Interview selected organizational personnel with personnel security responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the third-party personnel security control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>PS-8 PERSONNEL SANCTIONS</p> <p><u>Control:</u> The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.</p>	✓	✓	✓
PS-8.1	<i>Examine</i> organizational records or documents to determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	✓	✓	✓
PS-8.2	<i>Examine</i> organizational records or documents including signed rules of behavior to determine if the organization defines and conveys the formal sanctions process to organizational personnel.		✓	✓
PS-8.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the personnel sanctions control is implemented.		✓	✓
PS-8.4	<i>Interview</i> selected organizational personnel with personnel security responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently employs and monitors personnel sanctions on an ongoing basis.			✓
PS-8.5	<i>Interview</i> selected organizational personnel with personnel security responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the personnel sanctions control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

ASSESSMENT PROCEDURES

FAMILY: RISK ASSESSMENT

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>RA-1 RISK ASSESSMENT POLICY AND PROCEDURES</p> <p><u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.</p>	✓	✓	✓
RA-1.1	<p><i>Examine</i> organizational records or documents to determine if risk assessment 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.</p>	✓	✓	✓
RA-1.2	<p><i>Examine</i> the risk assessment policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</p>	✓	✓	✓
RA-1.3	<p><i>Examine</i> the risk assessment procedures to determine if the procedures are sufficient to address all areas identified in the risk assessment policy and all associated risk assessment controls.</p>		✓	✓
RA-1.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the risk assessment policy and procedures control is implemented.</p>		✓	✓
RA-1.5	<p><i>Examine</i> the risk assessment policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies, regulations, standards, and guidance.</p>			✓
RA-1.6	<p><i>Interview</i> selected organizational personnel with risk assessment responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies the risk assessment policy and procedures on an ongoing basis.</p>			✓
RA-1.7	<p><i>Interview</i> selected organizational personnel with risk assessment responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the risk assessment policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: RISK ASSESSMENT

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>RA-2 SECURITY CATEGORIZATION</p> <p><u>Control:</u> The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.</p>	✓	✓	✓
RA-2.1	<p><i>Examine the system security plan to determine if the security categorization of the information system: (i) exists; (ii) is consistent with FIPS 199; (iii) includes supporting rationale consistent with NIST Special Publication 800-60; and (iv) is reviewed and approved by designated senior-level officials within the organization.</i></p>	✓	✓	✓
RA-2.2	<p><i>Interview selected organizational personnel with risk assessment responsibilities to determine if the security categorization process is conducted as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and information owners.</i></p>	✓	✓	✓
RA-2.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security categorization control is implemented.</i></p>		✓	✓
RA-2.4	<p><i>Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if the organization consistently conducts security categorizations of the information system on an ongoing basis.</i></p>			✓
RA-2.5	<p><i>Interview selected organizational personnel with risk assessment responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security categorization control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: RISK ASSESSMENT

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>RA-3 RISK ASSESSMENT</p> <p><u>Control:</u> The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).</p>	✓	✓	✓
RA-3.1	<p><i>Examine</i> organizational records or documents to determine if the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties).</p>	✓	✓	✓
RA-3.2	<p><i>Examine</i> the risk assessment for the information system to determine if the assessment is consistent with NIST Special Publications 800-30 and 800-95.</p>	✓	✓	✓
RA-3.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the risk assessment control is implemented.</p>		✓	✓
RA-3.4	<p><i>Interview</i> selected organizational personnel with risk assessment responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts risk assessments for the information system on an ongoing basis.</p>			✓
RA-3.5	<p><i>Interview</i> selected organizational personnel with personnel security responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the risk assessment control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: RISK ASSESSMENT

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>RA-4 RISK ASSESSMENT UPDATE</p> <p><u>Control:</u> The organization updates the risk assessment [<i>Assignment: organization-defined frequency</i>] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.</p>	✓	✓	✓
RA-4.1	<p><i>Examine</i> organizational records or documents to determine if the risk assessment is updated in accordance with organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.</p>	✓	✓	✓
RA-4.2	<p><i>Examine</i> the risk assessment to determine if the report reflects the latest significant changes to the information system, the facilities where the system resides, or other conditions that may have impacted the security or accreditation status of the system.</p>		✓	✓
RA-4.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the risk assessment update control is implemented.</p>		✓	✓
RA-4.4	<p><i>Interview</i> selected organizational personnel with risk assessment responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently reviews and updates the risk assessment for the information system on an ongoing basis.</p>			✓
RA-4.5	<p><i>Interview</i> selected organizational personnel with risk assessment responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the risk assessment update control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: RISK ASSESSMENT

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	RA-5 VULNERABILITY SCANNING <u>Control:</u> The organization scans for vulnerabilities in the information system [Assignment: organization-defined frequency] or when significant new vulnerabilities affecting the system are identified and reported.		✓	✓
RA-5.1	<i>Examine</i> organizational records or documents to determine if the organization scans for vulnerabilities in the information system on an organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported.		✓	✓
RA-5.2	<i>Examine</i> the latest vulnerability scanning results to determine if the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans.		✓	✓
RA-5.3	<i>Examine</i> the latest vulnerability scanning results to determine if patch and vulnerability management is handled in accordance with NIST Special Publication 800-40 (Version 2).		✓	✓
RA-5.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the vulnerability scanning control is implemented.		✓	✓
RA-5.5	<i>Interview</i> selected organizational personnel with risk assessment responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently conducts vulnerability scanning of the information system on an ongoing basis.			✓
RA-5.6	<i>Interview</i> selected organizational personnel with risk assessment responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the vulnerability scanning control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	RA-5 VULNERABILITY SCANNING <u>Control Enhancement:</u> (1) Vulnerability scanning tools include the capability to readily update the list of information system vulnerabilities scanned.			✓
RA-5.7	<i>Interview</i> selected organizational personnel with risk assessment responsibilities to determine if the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned.			✓
RA-5.8	<i>Examine</i> previous vulnerability scan results to ensure that the tools used for vulnerability scanning include the capability to update the list of information system vulnerabilities scanned.			✓

FAMILY: RISK ASSESSMENT

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>RA-5 VULNERABILITY SCANNING Control Enhancement: (2) The organization updates the list of information system vulnerabilities scanned [Assignment: organization-defined frequency] or when significant new vulnerabilities are identified and reported.</p>			✓
RA-5.9	<p><i>Examine organizational records or documents to determine if the organization updates the list of information system vulnerabilities scanned on an organization-defined frequency or when significant new vulnerabilities are identified and reported.</i></p>			✓
	<p>RA-5 VULNERABILITY SCANNING Control Enhancement: (3) Vulnerability scanning procedures include means to ensure adequate scan coverage, both vulnerabilities checked and information system components scanned.</p>			
RA-5.10	<p><i>Examine organizational records or documents to determine if the organization provides adequate vulnerability scanning coverage including the key components of the information system (as defined by the organization) and the most up-to-date vulnerabilities.</i></p>			

ASSESSMENT PROCEDURES

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES <u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.</p>	✓	✓	✓
SA-1.1	<p><i>Examine</i> organizational records or documents to determine if system and services acquisition 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.</p>	✓	✓	✓
SA-1.2	<p><i>Examine</i> the system and services acquisition policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</p>	✓	✓	✓
SA-1.3	<p><i>Examine</i> the system and services acquisition procedures to determine if the procedures are sufficient to address all areas identified in the system and services acquisition policy and all associated system and services acquisition controls.</p>		✓	✓
SA-1.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system and services policy and procedures control is implemented.</p>		✓	✓
SA-1.5	<p><i>Examine</i> the system and services acquisition policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance.</p>			✓
SA-1.6	<p><i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies the system and services acquisition policy and procedures on an ongoing basis.</p>			✓

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

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
SA-1.7	<i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system and services acquisition policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

Draft

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SA-2 ALLOCATION OF RESOURCES</p> <p><u>Control:</u> The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.</p>	✓	✓	✓
SA-2.1	<p><i>Examine organizational records or documents to determine if the organization allocates, as part of its capital planning and investment control process, the resources required to adequately protect the information system consistent with NIST Special Publication 800-65.</i></p>	✓	✓	✓
SA-2.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the allocation of resources control is implemented.</i></p>		✓	✓
SA-2.3	<p><i>Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the organization consistently allocates sufficient resources to protect the information system on an ongoing basis.</i></p>			✓
SA-2.4	<p><i>Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the allocation of resources control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SA-3 LIFE CYCLE SUPPORT <u>Control:</u> The organization manages the information system using a system development life cycle methodology that includes information security considerations.	✓	✓	✓
SA-3.1	<i>Examine</i> organizational records or documents to determine if the organization manages the information system using a system development life cycle methodology that includes information security considerations.	✓	✓	✓
SA-3.2	<i>Examine</i> organizational records or documents to determine if the system development life cycle is consistent with NIST Special Publication 800-64.	✓	✓	✓
SA-3.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the life cycle support control is implemented.		✓	✓
SA-3.4	<i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently incorporates security considerations into the system development life cycle on an ongoing basis.			✓
SA-3.5	<i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the life cycle support control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SA-4 ACQUISITIONS <u>Control:</u> The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.</p>	✓	✓	✓
SA-4.1	<p><i>Examine</i> organizational records or documents to determine if system acquisition contracts include security requirements and/or security specifications based on an assessment of risk.</p>	✓	✓	✓
SA-4.2	<p><i>Examine</i> organizational records or documents to determine if the organization’s acquisition of commercial information technology products is consistent with NIST Special Publication 800-23.</p>		✓	✓
SA-4.3	<p><i>Examine</i> organizational records or documents to determine if references to security configuration settings and security implementation guidance in organizational acquisitions are consistent with NIST Special Publication 800-70.</p>		✓	✓
SA-4.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the acquisitions control is implemented.</p>		✓	✓
SA-4.5	<p><i>Examine</i> organizational records or documents to determine if acquisition contracts for information systems include, either explicitly or by reference, security requirements and/or security specifications that describe: (i) required security capabilities; (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation.</p>			✓
SA-4.6	<p><i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently includes security requirements and/or security specifications in information system acquisition contracts on an ongoing basis.</p>			✓
SA-4.7	<p><i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the acquisitions control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SA-5 INFORMATION SYSTEM DOCUMENTATION <u>Control:</u> The organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.	✓	✓	✓
SA-5.1	<i>Examine</i> organizational records or documents to determine if the organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.	✓	✓	✓
SA-5.2	<i>Examine</i> organizational records or documents to ensure that administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features.		✓	✓
SA-5.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system documentation control is implemented.		✓	✓
SA-5.4	<i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently provides, protects, and distributes information system documentation on an ongoing basis.			✓
SA-5.5	<i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system documentation control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	SA-5 INFORMATION SYSTEM DOCUMENTATION <u>Control Enhancement:</u> (1) The organization includes documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.		✓	✓
SA-5.6	<i>Examine</i> organizational records or documents to determine if the information system documentation describes the functional properties of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls.		✓	✓

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SA-5 INFORMATION SYSTEM DOCUMENTATION <u>Control Enhancement:</u> (2) The organization includes documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).</p>			✓
SA-5.7	<p><i>Examine organizational records or documents to determine if the information system documentation describes the design and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).</i></p>			✓

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SA-6 SOFTWARE USAGE RESTRICTIONS <u>Control:</u> The organization complies with software usage restrictions.</p>	✓	✓	✓
SA-6.1	<p><i>Examine</i> organizational records or documents to determine if the organization regularly reviews/analyzes software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.</p>	✓	✓	✓
SA-6.2	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the software usage restrictions control is implemented.</p>		✓	✓
SA-6.3	<p><i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently enforces software usage restrictions on an ongoing basis.</p>			✓
SA-6.4	<p><i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the software usage restrictions control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SA-7 USER INSTALLED SOFTWARE <u>Control:</u> The organization enforces explicit rules governing the downloading and installation of software by users.</p>	✓	✓	✓
SA-7.1	<p><i>Examine</i> organizational documents or records to determine if the organization enforces explicit rules regarding the downloading and installation of software by users.</p>	✓	✓	✓
SA-7.2	<p><i>Examine</i> organizational documents or records to determine if the organization regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.</p>	✓	✓	✓
SA-7.3	<p><i>Examine</i> firewall logs for indications that prohibited software is operational within the information system. (Note: applications tend to communicate on known ports and/or have signature traffic patterns and common packets.)</p>		✓	✓
SA-7.4	<p><i>Test</i> the enforcement of rules for user installed software on the information system by attempting to download and install (from an account with user privileges) software that is strictly prohibited; compare the results with a similar test conducted on an account with administrative privileges; determine which account rights violated the rules for user installed software.</p>		✓	✓
SA-7.5	<p><i>Test</i> network traffic on the information system to determine if prohibited software is installed and operational by utilizing a network packet analyzer. (Note: Applications tend to communicate on known ports and/or have signature traffic patterns and common packets.)</p>		✓	✓
SA-7.6	<p><i>Test</i> the information system for prohibited software by utilizing a scanner which detects and reports the names of installed software; compare the results against the approved software applications list.</p>		✓	✓
SA-7.7	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the user installed software control is implemented.</p>		✓	✓
SA-7.8	<p><i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently enforces rules for the downloading and installation of software by users on an ongoing basis.</p>			✓

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
SA-7.9	<i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the user installed software control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

Draft

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SA-8 SECURITY DESIGN PRINCIPLES <u>Control:</u> The organization designs and implements the information system using security engineering principles.		✓	✓
SA-8.1	<i>Examine</i> organizational records or documents to determine if the organization considers security design principles in the development and implementation of the information system consistent with NIST Special Publication 800-27.		✓	✓
SA-8.2	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security design principles control is implemented.		✓	✓
SA-8.3	<i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies security design principles in the development and implementation of organizational information systems on an ongoing basis.			✓
SA-8.4	<i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security design principles control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SA-9 OUTSOURCED INFORMATION SYSTEM SERVICES <u>Control:</u> The organization ensures that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance.</p>	✓	✓	✓
SA-9.1	<p><i>Examine</i> organizational records or documents to determine if the organization ensures that third-party providers of information system services employ adequate security controls in the information systems providing such services in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.</p>	✓	✓	✓
SA-9.2	<p><i>Examine</i> organizational records or documents to determine if the organization regularly reviews/analyzes outsourced information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.</p>		✓	✓
SA-9.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the outsourced information system services control is implemented.</p>		✓	✓
SA-9.4	<p><i>Examine</i> the security control assessment results from the organization providing outsourced information system services to determine if the security controls employed by third-party providers are compliant with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.</p>			✓
SA-9.5	<p><i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if third-party providers of information system services consistently employ adequate security controls in the information systems providing those services on an ongoing basis.</p>			✓
SA-9.6	<p><i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the outsourced information system services control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SA-10 DEVELOPER CONFIGURATION MANAGEMENT <u>Control:</u> The information system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.</p>			✓
SA-10.1	<p><i>Examine the information system developer configuration management plan to determine if the developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and the plan implementation.</i></p>			✓
SA-10.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the developer configuration management control is implemented.</i></p>			✓
SA-10.3	<p><i>Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if the information system developer consistently manages the information system configuration on an ongoing basis.</i></p>			✓
SA-10.4	<p><i>Interview selected organizational personnel with system and services acquisition responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the developer configuration management control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND SERVICES ACQUISITION

CLASS: MANAGEMENT

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SA-11 DEVELOPER SECURITY TESTING</p> <p><u>Control:</u> The information system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.</p>		✓	✓
SA-11.1	<i>Examine</i> the information system developer's organizational records or documents to determine if the developer creates a security test and evaluation plan, implements the plan, and documents the results.		✓	✓
SA-11.2	<i>Examine</i> organizational records or documents to determine if the organization includes the developer's security test and evaluation results in the organization's Plan of Action and Milestones.		✓	✓
SA-11.3	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the developer security testing control is implemented.		✓	✓
SA-11.4	<i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if the information system developer consistently implements security testing on an ongoing basis.			✓
SA-11.5	<i>Interview</i> selected organizational personnel with system and services acquisition responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the developer security testing control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

ASSESSMENT PROCEDURES

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES</p> <p><u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.</p>	✓	✓	✓
SC-1.1	<p><i>Examine organizational records or documents to determine if system and communications protection 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.</i></p>	✓	✓	✓
SC-1.2	<p><i>Examine the system and communications protection policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</i></p>	✓	✓	✓
SC-1.3	<p><i>Examine the system and communications protection procedures to determine if the procedures are sufficient to address all areas identified in the system and communications protection policy and all associated system and communications protection controls.</i></p>		✓	✓
SC-1.4	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system and communications protection policy and procedures control is implemented.</i></p>		✓	✓
SC-1.5	<p><i>Examine the system and communications protection policy to determine if the policy is consistent with the organization's mission, functions, and associated laws, directives, policies regulations, standards, and guidance.</i></p>			✓
SC-1.6	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the system and communications protection policy and procedures are consistently applied on an ongoing basis.</i></p>			✓

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

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
SC-1.7	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system and communications protection policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓

Draft

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-2 APPLICATION PARTITIONING <u>Control:</u> The information system separates user functionality (including user interface services) from information system management functionality.</p>		✓	✓
SC-2.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system physically and/or logically separates user functionality (including user interface services) from information system management functionality and how the separation is implemented and enforced.</i></p>		✓	✓
SC-2.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the application partitioning control is implemented.</i></p>		✓	✓
SC-2.3	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently implements application partitioning on an ongoing basis.</i></p>			✓
SC-2.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the application partitioning control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SC-3 SECURITY FUNCTION ISOLATION <u>Control:</u> The information system isolates security functions from nonsecurity functions.			✓
SC-3.1	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system isolates security functions from nonsecurity functions (including control of access to and integrity of the hardware, software, and firmware that perform those security functions) and how the system implements and enforces the isolation (e.g., partitions, domains, etc.).</i>			✓
SC-3.2	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security function isolation control is implemented.</i>			✓
SC-3.3	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system consistently implements security function isolation on an ongoing basis.</i>			✓
SC-3.4	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security function isolation control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓
	SC-3 SECURITY FUNCTION ISOLATION <u>Control Enhancement:</u> (1) The information system employs underlying hardware separation mechanisms to facilitate security function isolation.			
SC-3.5	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system employs hardware separation mechanisms to facilitate security function isolation.</i>			

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-3 SECURITY FUNCTION ISOLATION <u>Control Enhancement:</u> (2) The information system further divides the security functions with the functions enforcing access and information flow control isolated and protected from both nonsecurity functions and from other security functions.</p>			
SC-3.6	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.</i></p>			
	<p>SC-3 SECURITY FUNCTION ISOLATION <u>Control Enhancement:</u> (3) The information system minimizes the amount of nonsecurity functions included within the isolation boundary containing security functions.</p>			
SC-3.7	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.</i></p>			
	<p>SC-3 SECURITY FUNCTION ISOLATION <u>Control Enhancement:</u> (4) The information system security maintains its security functions in largely independent modules that avoid unnecessary interactions between modules.</p>			
SC-3.8	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system maintains its security functions in largely independent modules that avoid unnecessary interactions between modules.</i></p>			
	<p>SC-3 SECURITY FUNCTION ISOLATION <u>Control Enhancement:</u> (5) The information system security maintains its security functions in a layered structure minimizing interactions between layers of the design.</p>			
SC-3.9	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system security maintains its security functions in a layered structure minimizing interactions between layers of the design.</i></p>			

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-4 INFORMATION REMNANTS</p> <p><u>Control:</u> The information system prevents unauthorized and unintended information transfer via shared system resources.</p>		✓	✓
SC-4.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system prevents unauthorized and unintended information transfer via shared system resources and how the system prevents the transfer.</i></p>		✓	✓
SC-4.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information remnants control is implemented.</i></p>		✓	✓
SC-4.3	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system employs appropriate mechanisms to consistently prevent unauthorized and unintended transfer of information via shared system resources on an ongoing basis.</i></p>			✓
SC-4.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information remnants control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-5 DENIAL OF SERVICE PROTECTION <u>Control:</u> The information system protects against or limits the effects of the following types of denial of service attacks: [<i>Assignment: organization-defined list of types of denial of service attacks or reference to source for current list</i>].</p>	✓	✓	✓
SC-5.1	<p><i>Examine</i> organizational records or documents (including developer design documentation) to determine if the information system protects against or limits the effects of the organization-defined types of denial of service attacks.</p>	✓	✓	✓
SC-5.2	<p><i>Examine</i> organizational records or documents to determine if the organization uses automated tools to protect against or limit the effects of organization-defined types of denial of service attacks.</p>		✓	✓
SC-5.3	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the denial of service protection control is implemented.</p>		✓	✓
SC-5.4	<p><i>Test</i> the denial of service protection by simulating the launching of known denial of service/distributed denial of service attacks with automated tools (e.g. ping of death, teardrop, trinoo).</p>			✓
SC-5.5	<p><i>Interview</i> selected organizational personnel with system and communications protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently implements denial of service protection for the information system on an ongoing basis.</p>			✓
SC-5.6	<p><i>Interview</i> selected organizational personnel with system and communications protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the denial of service protection control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>SC-5 DENIAL OF SERVICE PROTECTION <u>Control Enhancement:</u> (1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.</p>			
SC-5.7	<p><i>Interview</i> selected organizational personnel with system and communications protection responsibilities and <i>examine</i> organizational records or documents (including developer design documentation) to determine if the information system restricts the ability of users to launch denial of service attacks against other information systems or networks.</p>			

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
SC-5.8	<i>Test the denial of service protection for the information system by simulating the launching of known denial of service/distributed denial of service attacks with automated tools (e.g. ping of death, teardrop, trinoo).</i>			
	<p>SC-5 DENIAL OF SERVICE PROTECTION <u>Control Enhancement:</u> (2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.</p>			
SC-5.9	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system limits the effects of information flooding types of denial of service attacks.</i>			
SC-5.10	<i>Test the denial of service protection for the information system by simulating the launching of known denial of service/distributed denial of service attacks with automated tools (e.g. ping of death, teardrop, trinoo).</i>			

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SC-6 RESOURCE PRIORITY <u>Control:</u> The information system limits the use of resources by priority.			
SC-6.1	<i>Examine</i> organizational records or documents (including developer design documentation) to determine if information system resources have been prioritized and how the system limits the use of resources by priority.			
SC-6.2	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that resource priority control is implemented.			
SC-6.3	<i>Interview</i> selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently limits the use of resources by priority on an ongoing basis.			
SC-6.4	<i>Interview</i> selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the resource priority control are documented and the resulting information used to actively improve the control on a continuous basis.			

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-7 BOUNDARY PROTECTION <u>Control:</u> The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.</p>	✓	✓	✓
SC-7.1	<p><i>Examine</i> organizational records or documents (including developer design documentation) to determine if the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.</p>	✓	✓	✓
SC-7.2	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the boundary protection control is implemented.</p>		✓	✓
SC-7.3	<p><i>Interview</i> selected organizational personnel with system and communications protection responsibilities and <i>examine</i> organizational records or documents to determine if the organization protects the boundaries of the information system using appropriate tools, techniques, and technologies on an ongoing basis.</p>			✓
SC-7.4	<p><i>Interview</i> selected organizational personnel with system and communications protection responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the boundary protection control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓
	<p>SC-7 BOUNDARY PROTECTION <u>Control Enhancement:</u> (1) The organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces. The organization prevents public access into the organization’s internal networks except as appropriately mediated.</p>		✓	✓
SC-7.5	<p><i>Interview</i> selected organizational personnel with system and communications protection responsibilities and <i>examine</i> organizational records or documents to determine if: (i) the organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces; and (ii) the organization prevents public access into the organization’s internal networks except as appropriately mediated.</p>		✓	✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SC-8 TRANSMISSION INTEGRITY <u>Control</u> : The information system protects the integrity of transmitted information.		✓	✓
SC-8.1	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system protects the integrity of transmitted information and how the integrity protections are implemented (i.e., mechanisms, tools, techniques, and technologies).</i>		✓	✓
SC-8.2	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that transmission integrity control is implemented.</i>		✓	✓
SC-8.3	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently protects the integrity of transmitted information on an ongoing basis.</i>			✓
SC-8.4	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the transmission integrity control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓
	SC-8 TRANSMISSION INTEGRITY <u>Control Enhancement</u> : (1) The organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).			✓
SC-8.5	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).</i>			✓
SC-8.6	<i>Examine organizational records or documents (including developer design documentation) to determine how the organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).</i>			✓
SC-8.7	<i>Test the cryptographic mechanisms employed in the information system used to achieve transmission integrity by attempting to exploit any known vulnerabilities.</i>			✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-9 TRANSMISSION CONFIDENTIALITY <u>Control:</u> The information system protects the confidentiality of transmitted information.</p>		✓	✓
SC-9.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system protects the confidentiality of transmitted information and how the confidentiality protections are implemented (i.e., mechanisms, tools, techniques, and technologies).</i></p>		✓	✓
SC-9.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the transmission confidentiality control is implemented.</i></p>		✓	✓
SC-9.3	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently protects the confidentiality of transmitted information on an ongoing basis.</i></p>			✓
SC-9.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the transmission confidentiality control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓
	<p>SC-9 TRANSMISSION CONFIDENTIALITY <u>Control Enhancement:</u> (1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).</p>			✓
SC-9.5	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).</i></p>			✓
SC-9.6	<p><i>Examine organizational records or documents (including developer design documentation) to determine how the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).</i></p>			✓

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

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
SC-9.7	<i>Test the cryptographic mechanisms employed in the information system used to achieve transmission confidentiality by attempting to exploit any known vulnerabilities.</i>			✓

Draft

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-10 NETWORK DISCONNECT</p> <p><u>Control:</u> The information system terminates a network connection at the end of a session or after [Assignment: organization-defined time period] of inactivity.</p>		✓	✓
SC-10.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system terminates a network connection at the end of a session or after an organization-defined time period of inactivity and how the connection is terminated.</i></p>		✓	✓
SC-10.2	<p><i>Test the network disconnection capability for the information system by leaving an open session for a specified amount of time to determine if the system terminates the network connection as expected.</i></p>		✓	✓
SC-10.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the network disconnect control is implemented.</i></p>		✓	✓
SC-10.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system consistently terminates network connections after an organization-defined period of inactivity on an ongoing basis.</i></p>			✓
SC-10.5	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the network disconnect control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-11 TRUSTED PATH</p> <p><u>Control:</u> The information system establishes a trusted communications path between the user and the security functionality of the system.</p>			
SC-11.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system establishes a trusted communications path between the user and the security functionality of the system and how the trusted path is implemented.</i></p>			
SC-11.2	<p><i>Test the information system trusted path by attempting to establish both a trusted and non-trusted communication path between the user and the security functionality of the system.</i></p>			
SC-11.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the trusted path control is implemented.</i></p>			
SC-11.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently implements a trusted communications path on an ongoing basis.</i></p>			
SC-11.5	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the trusted path control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT</p> <p><u>Control:</u> The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.</p>		✓	✓
SC-12.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and management and how the mechanisms and procedures are implemented.</i></p>		✓	✓
SC-12.2	<p><i>Test the information system cryptographic key establishment and management by using the automated mechanisms to walk a test key through all the phases of its lifecycle from generation to revocation.</i></p>		✓	✓
SC-12.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the cryptographic key establishment and management control is implemented.</i></p>		✓	✓
SC-12.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently employs automated mechanisms with supporting procedures or the organization employs manual procedures for cryptographic key establishment and management on an ongoing basis.</i></p>			✓
SC-12.5	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the cryptographic key establishment and management control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-13 USE OF VALIDATED CRYPTOGRAPHY</p> <p><u>Control:</u> When cryptography is employed within the information system, the cryptography complies with applicable federal laws, directives, policies, regulations, standards, and guidance, including FIPS 140-2 which requires the system to perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.</p>	✓	✓	✓
SC-13.1	<p><i>Examine organizational records or documents (including developer design documentation) to determine if the employed cryptography complies with applicable federal laws, directives, policies, regulations, standards, and guidance, including FIPS 140-2 which requires the system to perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.</i></p>	✓	✓	✓
SC-13.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the use of validated cryptography control is implemented.</i></p>		✓	✓
SC-13.3	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization consistently uses validated cryptography within the information system on an ongoing basis.</i></p>			✓
SC-13.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the use of validated cryptography control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SC-14 PUBLIC ACCESS PROTECTIONS <u>Control:</u> For publicly available systems, the information system protects the integrity of the information and applications.	✓	✓	✓
SC-14.1	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if, for publicly available information systems, the system protects the integrity of the information and applications and how the protections are implemented.</i>	✓	✓	✓
SC-14.2	<i>Test the publicly available information system by attempting to alter protected information using a public account to determine if access is limited in order to preserve the integrity of the information and the applications.</i>		✓	✓
SC-14.3	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the public access protections control is implemented.</i>		✓	✓
SC-14.4	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently protects the integrity of the information and applications on public access systems on an ongoing basis.</i>			✓
SC-14.5	<i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the public access protections control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-15 COLLABORATIVE COMPUTING <u>Control:</u> The information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone).</p>		✓	✓
SC-15.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone) and how remote activation of collaborative computing is prohibited.</i></p>		✓	✓
SC-15.2	<p><i>Test the information system by attempting to remotely control video or audio capabilities to determine if remote activation of collaborative computing mechanisms is restricted.</i></p>		✓	✓
SC-15.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the collaborative computing control is implemented.</i></p>		✓	✓
SC-15.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information systems consistently implements restrictions on the use of collaborative computing on an ongoing basis.</i></p>			✓
SC-15.5	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the collaborative computing control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓
	<p>SC-15 COLLABORATIVE COMPUTING <u>Control Enhancement:</u> (1) The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.</p>			
SC-15.6	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system provides physical disconnect of cameras and microphones in a manner that supports ease of use and how the information system provides physical disconnect of these components.</i></p>			

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-16 TRANSMISSION OF SECURITY PARAMETERS</p> <p><u>Control:</u> The information system reliably associates security parameters (e.g., security labels and markings) with information exchanged between information systems.</p>			
SC-16.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system associates security parameters (e.g., security labels and markings) with information exchanged between information systems and how the transmission of security parameters is implemented.</i></p>			
SC-16.2	<p><i>Test the information system's ability to associate security parameters between information systems by exchanging data between systems at different sensitivity levels.</i></p>			
SC-16.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the transmission of security parameters control is implemented.</i></p>			
SC-16.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system consistently transmits security parameters reliably between information systems on an ongoing basis.</i></p>			
SC-16.5	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the transmission of security parameters control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES <u>Control:</u> The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.</p>		✓	✓
SC-17.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system and how the policy is implemented in the information system.</i></p>		✓	✓
SC-17.2	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the public key infrastructure certificates control is implemented.</i></p>		✓	✓
SC-17.3	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization consistently develops and implements a certificate policy and certification practice statement for use in issuing public key certificates on an ongoing basis.</i></p>			✓
SC-17.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the public key infrastructure certificates control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-18 MOBILE CODE</p> <p><u>Control:</u> The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.</p>		✓	✓
SC-18.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; (ii) documents, monitors, and controls the use of mobile code within the information system; and (iii) requires organizational officials to approve the use of mobile code.</i></p>		✓	✓
SC-18.2	<p><i>Test the information system by attempting to run mobile code in an application where it is specifically prohibited to determine if the organization implements mobile code usage restrictions.</i></p>		✓	✓
SC-18.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the mobile code control is implemented.</i></p>		✓	✓
SC-18.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if mobile code is consistently restricted on an ongoing basis.</i></p>			✓
SC-18.5	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the mobile code control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-19 VOICE OVER INTERNET PROTOCOL</p> <p><u>Control:</u> The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) documents, monitors, and controls the use of VoIP within the information system. Appropriate organizational officials authorize the use of VoIP.</p>		✓	✓
SC-19.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization: (i) establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; (ii) documents, monitors, and controls the use of VoIP within the information system; and (iii) requires organizational officials to approve the use of VoIP.</i></p>		✓	✓
SC-19.2	<p><i>Test the VoIP capability by attempting to spoof or mask a caller's identity.</i></p>		✓	✓
SC-19.3	<p><i>Test the VoIP capability by attempting to generate enough network volume to create a denial of service attack.</i></p>		✓	✓
SC-19.4	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the VoIP control is implemented.</i></p>		✓	✓
SC-19.5	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the organization consistently manages VoIP technology by establishing usage restrictions and monitoring, documenting, and controlling the use of the technology within the information on an ongoing basis.</i></p>			✓
SC-19.6	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the VoIP control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-20 SECURE NAME LOOKUP SERVICE (AUTHORITATIVE SOURCE) <u>Control:</u> The information system (i.e., authoritative domain name servers) that provides the name lookup service for accessing organizational information resources to entities across the Internet provides artifacts for data origin authentication and data integrity to enable users to obtain message authentication and message integrity assurances for the information received during network-based transactions.</p>		✓	✓
SC-20.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system (i.e., authoritative domain name servers) that provides the name lookup service for accessing organizational information resources to entities across the Internet provides artifacts for data origin authentication and data integrity to enable users to obtain message authentication and message integrity assurances for the information received during network-based transactions and how the information system provides artifacts for data origin authentication and data integrity.</i></p>		✓	✓
SC-20.2	<p><i>Test the information system by attempting to launch known attacks against the domain name servers.</i></p>		✓	✓
SC-20.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the secure name lookup service (authoritative source) control is implemented.</i></p>		✓	✓
SC-20.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the secure name lookup service (authoritative source) is consistently implemented on an ongoing basis.</i></p>			✓
SC-20.5	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the secure name lookup service (authoritative source) control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-20 SECURE NAME LOOKUP SERVICE (AUTHORITATIVE SOURCE) Control Enhancement: (1) The information system verifies the authenticity of the artifacts for data origin authentication and data integrity (i.e., public key) of any subsidiary (child) zone in the name space in instances where the subsidiary (child) zone possesses this capability (i.e., provides these artifacts).</p>			
SC-20.6	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system verifies the authenticity of the artifacts for data origin authentication and data integrity (i.e., public key) of any subsidiary (child) zone in the name space in instances where the subsidiary (child) zone possesses this capability (i.e., provides these artifacts) and how the information system verifies the authenticity of the artifacts for data origin authentication and data integrity.</i></p>			

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-21 SECURE NAME LOOKUP SERVICE (RESOLUTION)</p> <p><u>Control:</u> The information system (i.e., authoritative domain name servers) that provides the name lookup service for accessing information resources to entities within the organization provides mechanisms for data origin authentication and data integrity verification and performs these services when requested by client systems.</p>			✓
SC-21.1	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents (including developer design documentation) to determine if the information system (i.e., authoritative domain name servers) that provides the name lookup service for accessing information resources to entities within the organization provides mechanisms for data origin authentication and data integrity verification and performs these services when requested by client systems and how the information system provides mechanisms for data origin authentication and data integrity verification.</i></p>			✓
SC-21.2	<p><i>Test the information system by attempting to launch known attacks against the domain name servers.</i></p>			✓
SC-21.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the secure name lookup service (resolution) control is implemented.</i></p>			✓
SC-21.4	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the secure name lookup service (resolution) is consistently implemented on an ongoing basis.</i></p>			✓
SC-21.5	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the secure name lookup service (resolution) control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

CLASS: TECHNICAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SC-21 SECURE NAME LOOKUP SERVICE (RESOLUTION) Control Enhancement: (1) The information system performs data origin authentication and data integrity verification for all information received whether or not client systems issue such requests.</p>			
SC-21.6	<p><i>Interview selected organizational personnel with system and communications protection responsibilities and examine organizational records or documents to determine if the information system performs data origin authentication and data integrity verification for all information received whether or not client systems issue such requests and how the information system performs data origin authentication and data integrity verification.</i></p>			

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

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES <u>Control:</u> The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, 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.	✓	✓	✓
SI-1.1	<i>Examine organizational records or documents 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.</i>	✓	✓	✓
SI-1.2	<i>Examine the system and information integrity policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.</i>	✓	✓	✓
SI-1.3	<i>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.</i>		✓	✓
SI-1.4	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the system and information integrity policy and procedures control is implemented.</i>		✓	✓
SI-1.5	<i>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.</i>			✓
SI-1.6	<i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently applies the system and information integrity policy and procedures on an ongoing basis.</i>			✓
SI-1.7	<i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the system and information integrity policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓

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

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SI-2 FLAW REMEDIATION <u>Control:</u> The organization identifies, reports, and corrects information system flaws.	✓	✓	✓
SI-2.1	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities to determine if the organization identifies recently announced software flaws and potential vulnerabilities resulting from those flaws that may affect the information system.	✓	✓	✓
SI-2.2	<i>Examine</i> organizational records or documents to determine if the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures.	✓	✓	✓
SI-2.3	<i>Interview</i> 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.		✓	✓
SI-2.4	<i>Examine</i> organizational records or documents to determine if the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation.		✓	✓
SI-2.5	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the flaw remediation control is implemented.		✓	✓
SI-2.6	<i>Examine</i> organizational records or documents to determine if the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.			✓
SI-2.7	<i>Test</i> the information system with automated security tools to determine the effectiveness of the organization's flaw remediation capabilities.			✓
SI-2.8	<i>Examine</i> organizational records or documents containing a listing/log of recent security flaw remediation actions performed on the information system to determine if the system is appropriately modified to reflect the required flaw remediation.			✓
SI-2.9	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies flaw remediation efforts within the information system on an ongoing basis.			✓

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
SI-2.10	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the flaw remediation control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	SI-2 FLAW REMEDIATION <u>Control Enhancement:</u> (1) The organization centrally manages the flaw remediation process and installs updates automatically without individual user intervention.			
SI-2.11	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities to determine if the organization centrally manages the flaw remediation process for the information system.			
SI-2.12	<i>Interview</i> 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.			
SI-2.13	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if the organization installs information system software updates automatically.			
SI-2.14	<i>Examine</i> the application that performs automatic updates to the information system software (or the documentation for the application) to determine how frequently automatic updates occur.			
	SI-2 FLAW REMEDIATION <u>Control Enhancement:</u> (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	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if the organization employs automated mechanisms to determine the security posture of information systems with respect to remediation of identified flaws.			

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SI-3 MALICIOUS CODE PROTECTION <u>Control:</u> The information system implements malicious code protection that includes a capability for automatic updates.	✓	✓	✓
SI-3.1	<i>Examine organizational records or documents to determine if the organization employs malicious code 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 to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses).</i>	✓	✓	✓
SI-3.2	<i>Interview selected organizational personnel with system and information integrity responsibilities and examine malicious code 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.</i>		✓	✓
SI-3.3	<i>Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization employs malicious code protection mechanisms for applications that may transfer malicious code (e.g., file transfer software, instant messaging software).</i>		✓	✓
SI-3.4	<i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational policy and procedures.</i>		✓	✓
SI-3.5	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the malicious code protection control is implemented.</i>		✓	✓
SI-3.6	<i>Examine malicious code protection mechanisms to determine if the mechanisms are: (i) appropriately updated to include the latest malicious code definitions; (ii) 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; and (iii) configured to disinfect and quarantine infected files.</i>			✓
SI-3.7	<i>Examine electronic mail clients and servers to determine if the clients and servers 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).</i>			✓

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
SI-3.8	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies malicious code protection measures within the information system on an ongoing basis.			✓
SI-3.9	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the malicious code protection control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	SI-3 MALICIOUS CODE PROTECTION <u>Control Enhancement:</u> (1) The organization centrally manages malicious code protection mechanisms.		✓	✓
SI-3.10	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if the organization centrally manages malicious code protection mechanisms employed in organizational information systems.		✓	✓
	SI-3 MALICIOUS CODE PROTECTION <u>Control Enhancement:</u> (2) The information system automatically updates malicious code protection mechanisms.			✓
SI-3.11	<i>Examine</i> the information system configuration to determine if the malicious code protection mechanisms are configured to download and install updates automatically directly from the vendor or some other trusted source.			✓

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES <u>Control:</u> The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.</p>		✓	✓
SI-4.1	<p><i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization employs information system monitoring tools and techniques to include intrusion detection systems, malicious code protection software, log monitoring software, and network forensic analysis tools.</i></p>		✓	✓
SI-4.2	<p><i>Examine intrusion detection tools for the information system to determine if the tools are configured and updated to detect vulnerabilities, changes to the network, both known and unknown attack signatures, and traffic anomalies.</i></p>		✓	✓
SI-4.3	<p><i>Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization is appropriately staffed and operational to monitor the information system in accordance with organizational policy and procedures.</i></p>		✓	✓
SI-4.4	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system monitoring tools and techniques control is implemented.</i></p>		✓	✓
SI-4.5	<p><i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently monitors the activity on the information system using appropriate monitoring tools and techniques on an ongoing basis.</i></p>			✓
SI-4.6	<p><i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information system monitoring tools and techniques control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓
	<p>SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES <u>Control Enhancement:</u> (1) The organization networks individual intrusion detection tools into a systemwide intrusion detection system using common protocols.</p>			
SI-4.7	<p><i>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.</i></p>			

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES <u>Control Enhancement:</u> (2) The organization employs automated tools to support near-real-time analysis of events in support of detecting system-level attacks.</p>			
SI-4.8	<p><i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization provides the capability through the employment of automated tools, to immediately investigate, report, and respond to suspicious activity in real-time.</i></p>			
	<p>SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES <u>Control Enhancement:</u> (3) 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.</p>			
SI-4.9	<p><i>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.</i></p>			
	<p>SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES <u>Control Enhancement:</u> (4) The information system monitors inbound and outbound communications for unusual or unauthorized activities indicating the presence of malware (e.g., malicious code, spyware, adware).</p>			
SI-4.10	<p><i>Examine organizational records or documents to determine if the information system monitors inbound and outbound communications for unusual or unauthorized activities indicating the presence of malware.</i></p>			
SI-4.11	<p><i>Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization reviews information system monitoring logs to assess if there is a pattern of unusual or unauthorized activities.</i></p>			

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SI-5 SECURITY ALERTS AND ADVISORIES <u>Control:</u> The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.</p>	✓	✓	✓
SI-5.1	<p><i>Examine organizational records or documents (including any logs documenting alerts/advisories) to determine if the organization: (i) receives information system security alerts and advisories; (ii) disseminates the alerts and advisories to appropriate personnel; (iii) takes appropriate actions in response; and (iv) documents the results including the date and time of each action taken.</i></p>	✓	✓	✓
SI-5.2	<p><i>Interview selected organizational personnel with system and information integrity responsibilities to determine if the organization provides the capability to immediately react and respond to new security alerts and advisories.</i></p>		✓	✓
SI-5.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security alerts and advisories control is implemented.</i></p>		✓	✓
SI-5.4	<p><i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently receives and responds to security alerts and advisories for the information system on an ongoing basis.</i></p>			✓
SI-5.5	<p><i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security alerts and advisories control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓
	<p>SI-5 SECURITY ALERTS AND ADVISORIES <u>Control Enhancement:</u> (1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.</p>			
SI-5.6	<p><i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization uses automated mechanisms to automatically disseminate security alerts and advisories to appropriate personnel and how the automated mechanisms are implemented.</i></p>			

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SI-6 SECURITY FUNCTIONALITY VERIFICATION <i>Control:</i> The information system verifies, to the extent feasible, the correct operation of security functions [<i>Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]</i>] and [<i>Selection (one or more): notifies system administrator, shuts the system down, restarts the system</i>] when anomalies are discovered.</p>			✓
SI-6.1	<p><i>Interview</i> 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.</p>			✓
SI-6.2	<p><i>Interview</i> 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.</p>			✓
SI-6.3	<p><i>Examine</i> the system configuration to determine if it verifies the correct operations of security functions [<i>Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]</i>] and [<i>Selection (one or more): notifies system administrator, shuts the system down, restarts the system</i>] when anomalies are discovered.</p>			✓
SI-6.4	<p><i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the security functionality verification control is implemented.</p>			✓
SI-6.5	<p><i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently verifies the security functionality within the system on an ongoing basis.</p>			✓
SI-6.6	<p><i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.</p>			✓

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SI-6 SECURITY FUNCTIONALITY VERIFICATION <u>Control Enhancement:</u> (1) The organization employs automated mechanisms to provide notification of failed security tests.</p>			
SI-6.7	<p><i>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 to appropriate personnel.</i></p>			
	<p>SI-6 SECURITY FUNCTIONALITY VERIFICATION <u>Control Enhancement:</u> (2) The organization employs automated mechanisms to support management of distributed security testing.</p>			
SI-6.8	<p><i>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.</i></p>			

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SI-7 SOFTWARE AND INFORMATION INTEGRITY <u>Control:</u> The information system detects and protects against unauthorized changes to software and information.			✓
SI-7.1	<i>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.</i>			✓
SI-7.2	<i>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).</i>			✓
SI-7.3	<i>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.</i>			✓
SI-7.4	<i>Examine information system integrity applications and tools to determine if the applications and tools effectively detect unauthorized changes to software and information.</i>			✓
SI-7.5	<i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the software and information integrity control is implemented.</i>			✓
SI-7.6	<i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system detects and protects against unauthorized changes to software and information on an ongoing basis.</i>			✓
SI-7.7	<i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the software and information integrity control are documented and the resulting information used to actively improve the control on a continuous basis.</i>			✓

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SI-8 SPAM PROTECTION <u>Control:</u> The information system implements spam protection.		✓	✓
SI-8.1	<i>Examine</i> organizational records or documents to determine if the organization employs spam 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.		✓	✓
SI-8.2	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if the organization employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail.		✓	✓
SI-8.3	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if the organization updates spam protection mechanisms whenever new releases are available in accordance with organizational policy and procedures.		✓	✓
SI-8.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the spam protection control is implemented.		✓	✓
SI-8.5	<i>Examine</i> the information system’s spam protection mechanism(s) by scanning critical information system entry points for the presence of spam.			✓
SI-8.6	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if the organization consistently applies spam protection measures within the information system on an ongoing basis.			✓
SI-8.7	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the spam protection control are documented and the resulting information used to actively improve the control on a continuous basis.			✓
	SI-8 SPAM PROTECTION <u>Control Enhancement:</u> (1) The organization centrally manages spam protection mechanisms.			✓
SI-8.8	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if the organization employs a centralized management architecture to manage spam protection mechanisms for the information system.			✓

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SI-8 SPAM PROTECTION Control Enhancement: (2) The information system automatically updates spam protection mechanisms.			
SI-8.9	<i>Examine spam protection mechanisms to determine if the mechanisms are configured to download and install updates automatically from the vendor or some other trusted source.</i>			

Draft

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SI-9 INFORMATION INPUT RESTRICTIONS <u>Control:</u> The organization restricts the information input to the information system to authorized personnel only.</p>		✓	✓
SI-9.1	<p><i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the information system employs restrictions on personnel authorized to input information to the information system to include limitations based on specific operational/project responsibilities.</i></p>		✓	✓
SI-9.2	<p><i>Examine the information system to determine if user accounts are restricted from inputting information beyond the typical access controls unless specifically authorized based on operational/project responsibilities.</i></p>		✓	✓
SI-9.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information input restrictions control is implemented.</i></p>		✓	✓
SI-9.4	<p><i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently restricts information system inputs to the information system on an ongoing basis.</i></p>			✓
SI-9.5	<p><i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information input restrictions control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY <u>Control:</u> The information system checks information for accuracy, completeness, validity, and authenticity.		✓	✓
SI-10.1	<i>Examine</i> 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.		✓	✓
SI-10.2	<i>Examine</i> 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.		✓	✓
SI-10.3	<i>Examine</i> the information system to determine if the system prescreens inputs passed to interpreters to ensure the content is not unintentionally interpreted as commands.		✓	✓
SI-10.4	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information accuracy, completeness, validity, and authenticity control is implemented.		✓	✓
SI-10.5	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently performs information accuracy, completeness, validity, and authenticity checks on an ongoing basis.			✓
SI-10.6	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the security functionality verification control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	SI-11 ERROR HANDLING <u>Control:</u> The information system identifies and handles error conditions in an expeditious manner.		✓	✓
SI-11.1	<i>Examine</i> the information system to determine if the system identifies and handles error conditions in an expeditious manner.		✓	✓
SI-11.2	<i>Examine</i> the information system to determine if the system provides timely error messages that contain useful information to users without revealing information that could be exploited by adversaries.		✓	✓
SI-11.3	<i>Examine</i> the information system to determine if the system provides error messages only to authorized personnel (e.g., system administrators, maintenance personnel).		✓	✓
SI-11.4	<i>Examine</i> the information system to determine if the system lists sensitive information (e.g., account numbers, social security numbers, and credit card numbers) in error logs or associated administrative messages.		✓	✓
SI-11.5	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities to determine if the information system provides the capability to identify and handle error conditions in compliance with organizational policy and procedures.		✓	✓
SI-11.6	<i>Examine</i> organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the error handling control is implemented.		✓	✓
SI-11.7	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if the information system consistently handles error conditions on an ongoing basis.			✓
SI-11.8	<i>Interview</i> selected organizational personnel with system and information integrity responsibilities and <i>examine</i> organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the error handling control are documented and the resulting information used to actively improve the control on a continuous basis.			✓

FAMILY: SYSTEM AND INFORMATION INTEGRITY

CLASS: OPERATIONAL

STEP NUMBER	ASSESSMENT PROCEDURE	LOW	MODERATE	HIGH
	<p>SI-12 INFORMATION OUTPUT HANDLING AND RETENTION</p> <p><u>Control:</u> The organization handles and retains output from the information system in accordance with organizational policy and operational requirements.</p>		✓	✓
SI-12.1	<p><i>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.</i></p>		✓	✓
SI-12.2	<p><i>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.</i></p>		✓	✓
SI-12.3	<p><i>Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information output handling and retention control is implemented.</i></p>		✓	✓
SI-12.4	<p><i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if the organization consistently handles and retains information output from the information system on an ongoing basis.</i></p>			✓
SI-12.5	<p><i>Interview selected organizational personnel with system and information integrity responsibilities and examine organizational records or documents to determine if anomalies or problems encountered by the organization in the implementation of the information output handling and retention control are documented and the resulting information used to actively improve the control on a continuous basis.</i></p>			✓

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 (i.e., low, moderate, and high) and by assessment method (i.e., examine, interview, and test). Within assessment method, the procedures are further grouped by closely related control topics (e.g., backup and recovery [CP-9 and CP-10 respectively]) and objects assessed (e.g., records and documents, alternate storage sites). The identifier in brackets (e.g., [CP-5.1]) following each procedural statement corresponds to the 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. Organizations may have also applied the tailoring guidance from NIST Special Publication 800-53 to eliminate or downgrade selected security controls or employ 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: Examine**CP-1 (Policy and Procedures)**

Examine organizational records or documents, the contingency planning policy, the contingency plan procedures, and the contingency plan to determine:

(1) 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-1.1]

(2) if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance. [CP-1.2]

CP-2, CP-5 (Contingency Plan and Contingency Plan Update)

Examine organizational records or documents and the contingency plan to determine:

(1) if a contingency plan:

- (i) exists;
- (ii) is documented;
- (iii) is disseminated to appropriate elements within the organization; and
- (iv) is reviewed and approved by responsible officials within the organization; [CP-2.1]

(2) if the plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system in accordance with NIST Special Publication 800-34 and [CP-2.2]

(3) if the contingency plan is updated in accordance with organization defined frequency, at least annually. [CP-5.1]

CP-9, CP-10 (Information System Backup & Recovery)

Examine organizational records or documents to determine:

(1) if the organization defines the user-level and system-level information (including system state information) that is require to be backed up and identifies the location for storing backup information; and [CP-9.1]

(2) if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system. [CP-10.1]

Examine selected information backup media, or selected records of backups if available, to determine if the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency and stores the backup information in designated locations in accordance with information system backup procedures. [CP-9.2]

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

LOW-IMPACT INFORMATION SYSTEMS

ASSESSMENT METHOD: Interview

No procedural statements.

Draft

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

LOW-IMPACT INFORMATION SYSTEMS

ASSESSMENT METHOD: Test

No procedural statements.

Draft

FAMILY: CONTINGENCY PLANNING**CLASS: OPERATIONAL**

MODERATE-IMPACT INFORMATION SYSTEMS

ASSESSMENT METHOD: Examine**CP-1 (Policy and Procedures)**

Examine organizational records or documents, the contingency planning policy, the contingency plan procedures, and the contingency plan to determine:

- (1) 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-1.1]
- (2) if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; [CP-1.2]
- (3) if the procedures are sufficient to address all areas identified in the contingency planning policy and all associated contingency planning controls; and [CP-1.3]
- (4) if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency planning policy and procedures control is implemented. [CP-1.4]

CP-2, CP-5 (Contingency Plan and Contingency Plan Update)

Examine organizational records or documents and the contingency plan to determine:

- (1) if a contingency plan:
 - (i) exists;
 - (ii) is documented;
 - (iii) is disseminated to appropriate elements within the organization; and
 - (iv) is reviewed and approved by responsible officials within the organization. [CP-2.1]
- (2) if the plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system in accordance with NIST Special Publication 800-34. [CP-2.2]
- (3) if the contingency plan is updated in accordance with organization defined frequency, at least annually. [CP-5.1]
- (4) if the revised plan reflects the needed changes based upon the organization's experiences during plan implementation, execution, and testing; [CP-5.2]
- (5) if the organization assigns responsibility to specific parties and defines specific actions to ensure that:
 - (i) the contingency plan control is implemented; and [CP-2.4]
 - (ii) contingency plan update control is implemented. [CP-5.3]
- (6) if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan) and if the contingency plan supports the requirements in the related plans. [CP-2.7]

CP-3 (Training)

Examine organizational records or documents to determine:

- (1) if the organization identifies personnel with significant contingency roles and responsibilities and documents those roles and responsibilities; [CP-3.1]

(2) if the organization:

- (i) provides contingency training to personnel with significant contingency roles and responsibilities or personnel implementing the contingency plan;
- (ii) records the type of contingency training received and the date completed; and
- (iii) provides initial and refresher training in accordance with organization-defined frequency, at least annually; and [CP-3.2]

(3) if the organization assigns responsibility to specific parties and defines specific actions to ensure that contingency training control is implemented. [CP-3.4]

Examine the contingency training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities. [CP-3.3]

CP-4 (Contingency Plan Testing)

Examine organizational records or documents to determine:

(1) if the organization tests its contingency plan using the organization-defined tests and exercises in accordance with the organization-defined frequency and documents the results of the tests; [CP-4.1]

(2) if the contingency plan test results are reviewed and if corrective actions are being taken; [CP-4.2]

(3) 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-4.3]

(4) if the organization assigns responsibility to specific parties and defines specific actions to ensure that contingency plan testing control is implemented; and [CP-4.4]

(5) if 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-4.8]

CP-6, CP-7 (Alternate Storage and Alternate Processing)

Examine organizational records or documents to determine:

(1) if alternate storage site agreements are currently in place to permit storage of information system backup information; [CP-6.1]

(2) if alternate processing site 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]

(3) if the organization assigns responsibility to specific parties and defines specific actions to ensure that alternate storage site control is implemented; [CP-6.2]

(4) if the organization assigns responsibility to specific parties and defines specific actions to ensure that alternate processing site control is implemented. [CP-7.2]

Examine the contingency plan to determine if the plan:

(1) identifies the primary storage site hazards; [CP-6.6]

(2) identifies the primary processing site hazards; and [CP-7.6]

(3) identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and defines explicit mitigation actions for those accessibility problems. [CP-7.8]

Examine the 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 site. [CP-6.7]

Examine the 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 site. [CP-7.7]

Examine alternate processing site agreements to determine if the agreements contain priority of service provisions in accordance with the organization's availability requirements. [CP-7.9]

CP-8 (Telecommunication Services)

Examine primary and alternate telecommunication service agreements to determine:

- (1) 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]
- (2) if the agreements contain priority of service provisions in accordance with the availability requirements defined in the organization's contingency plan; and [CP-8.5]
- (3) if the alternate and primary telecommunication services share a single point of failure. [CP-8.6]

Examine organizational records or documents to determine if the organization assigns responsibility to specific parties and defines specific actions to ensure the telecommunications services control is implemented. [CP-8.2]

CP-9, CP-10 (Information System Backup and Recovery)

Examine organizational records or documents to determine:

- (1) if the organization defines the user-level and system-level information (including system state information) that is required to be backed up and identifies the location for storing backup information; [CP-9.1]
- (2) if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system; [CP-10.1]
- (3) if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system backup control is implemented; [CP-9.3]
- (4) if the organization identifies means for capturing the information system's operational state including all system parameters, patches, configuration settings, and application/system software prior to system disruption or failure; [CP-10.2]
- (5) if the organization tests the information system after completion of recovery and reconstitution operations; and [CP-10.3]
- (6) if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system recovery and reconstitution control is implemented. [CP-10.4]

Examine selected information backup media, or selected records of backups if available, to determine if the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency and stores the backup information in designated locations in accordance with information system backup procedures. [CP-9.2]

Examine organizational records or documents including results from testing of backup operations to determine if the organization conducts testing within the organization-defined frequency, and if the testing results indicate backup media reliability and information integrity. [CP-9.6]

FAMILY: CONTINGENCY PLANNING**CLASS:** OPERATIONAL

MODERATE-IMPACT INFORMATION SYSTEMS

ASSESSMENT METHOD: Interview**CP-2 (Contingency Plan)**

***Interview** selected organizational personnel with contingency planning and plan implementation responsibilities to determine if key operating elements within the organization understand the contingency plan and are ready to implement the plan. [CP-2.3]*

CP-8 (Telecommunication Services)

***Interview** appropriate telecommunications service providers to determine if alternate and primary telecommunications services share a single point of failure. [CP-8.6]*

Draft

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

MODERATE-IMPACT INFORMATION SYSTEMS

ASSESSMENT METHOD: Test

No procedural statements.

Draft

FAMILY: CONTINGENCY PLANNING**CLASS: OPERATIONAL**

HIGH-IMPACT INFORMATION SYSTEMS

ASSESSMENT METHOD: Examine**CP-1 (Policy and Procedures)**

Examine organizational records or documents, the contingency planning policy, the contingency plan procedures, and the contingency plan to determine:

- (1) 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-1.1]
- (2) if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; [CP-1.2]
- (3) if the procedures are sufficient to address all areas identified in the contingency planning policy and all associated contingency planning controls; [CP-1.3]
- (4) if the organization assigns responsibility to specific parties and defines specific actions to ensure that the contingency planning policy and procedures control is implemented; [CP-1.4]
- (5) if the organization consistently applies the contingency planning policy and procedures on an ongoing basis; and [CP-1.6]
- (6) if anomalies or problems encountered by the organization in the implementation of the contingency planning policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis. [CP-1.7]

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-1.5]

CP-2, CP-5 (Contingency Plan and Contingency Plan Update)

Examine organizational records or documents and the contingency plan to determine:

- (1) if a contingency plan:
 - (i) exists;
 - (ii) is documented;
 - (iii) is disseminated to appropriate elements within the organization; and
 - (iv) is reviewed and approved by responsible officials within the organization. [CP-2.1]
- (2) if the plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system in accordance with NIST Special Publication 800-34. [CP-2.2]
- (3) if the contingency plan is updated in accordance with organization defined frequency, at least annually; [CP-5.1]
- (4) if the revised plan reflects the needed changes based upon the organization's experiences during plan implementation, execution, and testing; [CP- 5.2]
- (5) if the organization assigns responsibility to specific parties and defines specific actions to ensure that:
 - (i) the contingency plan control is implemented; and [CP-2.4]
 - (ii) contingency plan update control is implemented. [CP-5.3]

(6) if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan) and if the contingency plan supports the requirements in the related plans; [CP-2.7]

(7) if designated officials within the organization consistently review and approve the contingency plan and distribute the plan to key contingency personnel on an ongoing basis; [CP-2.5]

(8) if anomalies or problems encountered by the organization in the implementation of the contingency plan control are documented and the resulting information used to actively improve the control on a continuous basis; [CP-2.6]

(9) if the organization consistently reviews and updates the contingency plan on an ongoing basis; and [CP-5.4]

(10) if anomalies or problems encountered by the organization in the implementation of the contingency plan update control are documented and the resulting information used to actively improve the control on a continuous basis. [CP-5.5]

CP-3 (Training)

Examine organizational records or documents to determine:

(1) if the organization identifies personnel with significant contingency roles and responsibilities and documents those roles and responsibilities; [CP-3.1]

(2) if the organization:

(i) provides contingency training to personnel with significant contingency roles and responsibilities or personnel implementing the contingency plan;

(ii) records the type of contingency training received and the date completed; and

(iii) provides initial and refresher training in accordance with organization-defined frequency, at least annually; and [CP-3.2]

(3) if the organization assigns responsibility to specific parties and defines specific actions to ensure that contingency training control is implemented; [CP-3.4]

(4) if the organization simulates contingency training events; [CP-3.7]

(5) if the organization conducts contingency plan testing at the alternate processing site to familiarize contingency personnel with the facility and its resources and to evaluate the site's capabilities to support contingency operations; [CP-4.9]

(6) if the organization consistently conducts contingency training on an ongoing basis; and [CP-3.5]

(7) if anomalies or problems encountered by the organization in the implementation of the contingency training control are documented and the resulting information used to actively improve the control on a continuous basis. [CP-3.6]

Examine the contingency training material for the selected roles and responsibilities to determine if the material addresses the procedures and activities necessary to fulfill those roles and responsibilities. [CP-3.3]

CP-4 (Contingency Plan Testing)

Examine organizational records or documents to determine:

(1) if the organization tests its contingency plan using the organization-defined tests and exercises in accordance with the organization-defined frequency and documents the results of the tests; [CP-4.1]

(2) if the contingency plan test results are reviewed and if corrective actions are being taken; [CP-4.2]

(3) 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-4.3]

(4) if the organization assigns responsibility to specific parties and defines specific actions to ensure that contingency plan testing control is implemented; [CP-4.4]

(5) if 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-4.8]

(6) if the organization consistently conducts contingency plan testing on an ongoing basis; [CP-4.6]

(7) if anomalies or problems encountered by the organization in the implementation of the contingency plan testing control are documented and the resulting information used to actively improve the control on a continuous basis; and [CP-4.7]

Examine organizational records or documents to determine if the organization conducts contingency plan testing at the alternate processing site to familiarize contingency personnel with the facility and its resources and to evaluate the site's capabilities to support contingency operations. [CP-4.9]

CP-6, CP-7 (Alternate Storage and Alternate Processing)

Examine organizational records or documents to determine:

(1) if alternate storage site agreements are currently in place to permit storage of information system backup information; [CP-6.1]

(2) if alternate processing site 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]

(3) if the organization assigns responsibility to specific parties and defines specific actions to ensure that alternate storage site control is implemented; [CP-6.2]

(4) if the organization assigns responsibility to specific parties and defines specific actions to ensure that alternate processing site control is implemented; [CP-7.2]

(5) if the organization consistently reviews and updates alternate storage site agreements on an ongoing basis; and [CP-6.4]

(6) if anomalies or problems encountered by the organization in the implementation of the alternate storage sites control are documented and the resulting information used to actively improve the control on a continuous basis; [CP-6.5]

(7) if the organization consistently reviews and updates alternate processing site agreements on an ongoing basis; and [CP-7.4]

(8) if anomalies or problems encountered by the organization in the implementation of the alternate processing sites control are documented and the resulting information used to actively improve the control on a continuous basis. [CP-7.5]

Examine the contingency plan to determine if the plan:

(1) identifies the primary storage site hazards; [CP-6.6]

(2) identifies the primary processing site hazards; [CP-7.6]

(3) identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and defines explicit mitigation actions for those accessibility problems; and [CP-7.8]

(4) 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. [CP-6.10]

Examine the alternate storage site to determine:

(1) if the site is available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup information; and [CP6.3]

(2) 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 site. [CP-6.7]

Examine the alternate storage site agreement to determine if the agreement specifies requirements to facilitate timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives). [CP-6.8]

Examine the alternate processing site to determine:

(1) 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 site; and [CP-7.7]

(2) 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-7.3]

Examine alternate processing site agreements to determine:

(1) if the agreements contain priority of service provisions in accordance with the organization's availability requirements; and [CP-7.9]

(2) if the agreements specify the requirements needed to support the minimum required operational capability of the organization. [CP-7.10]

CP-8 (Telecommunication Services)

Examine primary and alternate telecommunication service agreements to determine:

(1) 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]

(2) if the agreements contain priority of service provisions in accordance with the availability requirements defined in the organization's contingency plan; and [CP-8.5]

(3) if the alternate and primary telecommunication services share a single point of failure. [CP-8.6]

Examine organizational records or documents to determine:

(1) if the organization assigns responsibility to specific parties and defines specific actions to ensure the telecommunications services control is implemented; [CP-8.2]

(2) if the organization consistently reviews primary and alternate telecommunications service agreements on an ongoing basis; and [CP-8.3]

(3) if anomalies or problems encountered by the organization in the implementation of the telecommunications services control are documented and the resulting information used to actively improve the control on a continuous basis. [CP-8.4]

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 site. [CP-8.7]

Examine the contingency plans from the primary and alternate telecommunication service providers to determine if the contingency plans are adequate. [CP-8.8]

CP-9, CP-10 (Information System Backup and Recovery)

Examine organizational records or documents to determine:

(1) if the organization defines the user-level and system-level information (including system state information) that is require to be backed up and identifies the location for storing backup information; [CP-9.1]

(2) if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system; [CP-10.1]

(3) if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system backup control is implemented; [CP-9.3]

(4) if the organization identifies means for capturing the information system's operational state including all system parameters, patches, configuration settings, and application/system software prior to system disruption or failure; [CP-10.2]

(5) if the organization tests the information system after completion of recovery and reconstitution operations; [CP-10.3]

(6) if the organization assigns responsibility to specific parties and defines specific actions to ensure that the information system recovery and reconstitution control is implemented; [CP-10.4]

(7) if the organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing and if the use of the backup information contributes to a successful restoration of the identified functions within the information system; [CP-9.7]

(8) if the organization consistently conducts information system backups on an ongoing basis; [CP-9.4]

(9) if anomalies or problems encountered by the organization in the implementation of the information system backup control are documented and the resulting information used to actively improve the control on a continuous basis; [CP-9.5]

(10) if the organization consistently conducts recovery and reconstitution operations on an ongoing basis; and [CP-10.6]

(11) if anomalies or problems encountered by the organization in the implementation of the information system recovery and reconstitution control are documented and the resulting information used to actively improve the control on a continuous basis. [CP-10.7]

Examine selected information backup media, or selected records of backups if available, to determine if the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency and stores the backup information in designated locations in accordance with information system backup procedures. [CP-9.2]

Examine organizational records or documents including results from testing of backup operations to determine if the organization conducts testing within the organization-defined frequency, and if the testing results indicate backup media reliability and information integrity. [CP-9.6]

Examine the storage location for backup copies of the operating system and other critical information system software to determine if the backup copies of the software are stored in a separate facility or in a fire-rated container that is not collocated with the operational software. [CP-9.8]

Examine organizational records or documents including results from contingency plan testing to determine if the organization includes a full recovery and reconstitution of the information system as part of contingency plan testing. [CP-10.8]

FAMILY: CONTINGENCY PLANNING**CLASS: OPERATIONAL**

HIGH-IMPACT INFORMATION SYSTEMS

ASSESSMENT METHOD: Interview**CP-1 (Policy and Procedures)**

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

(1) if the organization consistently applies the contingency planning policy and procedures on an ongoing basis; and [CP-1.6]

(2) if anomalies or problems encountered by the organization in the implementation of the contingency planning policy and procedures control are documented and the resulting information used to actively improve the control on a continuous basis. [CP-1.7]

CP-2, CP-5 (Contingency Plan and Contingency Plan Update)

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

(1) if key operating elements within the organization understand the contingency plan and are ready to implement the plan; [CP-2.3]

(2) if designated officials within the organization consistently review and approve the contingency plan and distribute the plan to key contingency personnel on an ongoing basis; [CP-2.5]

(3) if anomalies or problems encountered by the organization in the implementation of the contingency plan control are documented and the resulting information used to actively improve the control on a continuous basis; [CP-2.6]

(4) if the organization consistently reviews and updates the contingency plan on an ongoing basis; and [CP-5.4]

(5) if anomalies or problems encountered by the organization in the implementation of the contingency plan update control are documented and the resulting information used to actively improve the control on a continuous basis. [CP-5.5]

CP-3 (Training)

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

(1) if the organization consistently conducts contingency training on an ongoing basis; [CP-3.5]

(2) if anomalies or problems encountered by the organization in the implementation of the contingency training control are documented and the resulting information used to actively improve the control on a continuous basis; and [CP-3.6]

(3) how the organization uses simulated events to improve the training process. [CP-3.8]

CP-4 (Contingency Plan Testing)

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

(1) the overall effectiveness of the contingency plan and the readiness of the organization to execute the plan; [CP-4.5]

(2) if the organization consistently conducts contingency plan testing on an ongoing basis; and [CP-4.6]

(3) if anomalies or problems encountered by the organization in the implementation of the contingency plan testing control are documented and the resulting information used to actively improve the control on a continuous basis. [CP-4.7]

CP-6, CP-7 (Alternate Storage and Alternate Processing)

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

(1) if the organization consistently reviews and updates alternate storage site agreements on an ongoing basis; [CP-6.4]

(2) if anomalies or problems encountered by the organization in the implementation of the alternate storage sites control are documented and the resulting information used to actively improve the control on a continuous basis; [CP-6.5]

(3) if the organization consistently reviews and updates alternate processing site agreements on an ongoing basis; and [CP-7.4]

(4) if anomalies or problems encountered by the organization in the implementation of the alternate processing sites control are documented and the resulting information used to actively improve the control on a continuous basis. [CP-7.5]

CP-8 (Telecommunication Services)

Interview appropriate telecommunications service providers to determine if alternate and primary telecommunications services share a single point of failure. [CP-8.6]

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

(1) if the organization consistently reviews primary and alternate telecommunications service agreements on an ongoing basis; and [CP-8.3]

(2) if anomalies or problems encountered by the organization in the implementation of the telecommunications services control are documented and the resulting information used to actively improve the control on a continuous basis. [CP-8.4]

CP-9, CP-10 (Information System Backup and Recovery)

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

(1) if the organization consistently conducts information system backups on an ongoing basis; [CP-9.4]

(2) if anomalies or problems encountered by the organization in the implementation of the information system backup control are documented and the resulting information used to actively improve the control on a continuous basis; [CP-9.5]

(3) if the organization consistently conducts recovery and reconstitution operations on an ongoing basis; and [CP-10.6]

(4) if anomalies or problems encountered by the organization in the implementation of the information system recovery and reconstitution control are documented and the resulting information used to actively improve the control on a continuous basis. [CP-10.7]

FAMILY: CONTINGENCY PLANNING**CLASS:** OPERATIONAL

HIGH-IMPACT INFORMATION SYSTEMS

ASSESSMENT METHOD: Test**CP-3 (Training)**

Test selected simulated events to determine if organizational personnel respond as expected to the simulated crisis situation. [CP-3.9]

CP-6, CP-7 (Alternate Storage and Processing)

Test the alternate storage site operations to determine if the 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-6.9]

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]

CP-9, CP-10 (Information System Backup and Recovery)

Test 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. [CP-10.5]

APPENDIX H

MINIMUM ASSESSMENT PROCEDURES – SUMMARY

LOW-IMPACT, MODERATE-IMPACT, AND HIGH-IMPACT INFORMATION SYSTEMS

The following table provides a summary of the minimum assessment procedures for low-impact, moderate-impact, and high-impact information systems as defined in Appendix F. The minimum assessment procedures are based on the minimum security controls defined in NIST Special Publication 800-53 in accordance with the low, moderate, and high security control baselines. For each security control and security control enhancement listed in the three security control baselines, the appropriate minimum procedural statements required to assess the effectiveness of the control or control enhancement are listed in the table. For example, the minimum procedural statements required to assess the effectiveness of security control CP-2 in the low baseline are CP-2.1 and CP-2.2. For the moderate baseline, the minimum procedural statements required to assess the effectiveness of security control CP-2 are CP-2.1, CP-2.2, CP-2.3, and CP-2.4. For the high baseline, the minimum procedural statements required to assess the effectiveness of security control CP-2 are CP-2.1, CP-2.2, CP-2.3, CP-2.4, CP-2.5, and CP-2.6. To assess the effectiveness of the first enhancement to security control CP-2, which appears in both the moderate and high baselines, the minimum procedural statement required is CP-2.7. The *not applicable* entries in the table indicate that there are no minimum assessment procedural statements for the security control or security control enhancement because the control or enhancement does not appear in the particular security control baseline. There are additional procedural statements in the master catalog of assessment procedures in Appendix F that are not listed in the table but are available to assessors to increase the level of assurance in the effectiveness of the security controls employed in the information system.

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
Access Control				
AC-1	Access Control Policy and Procedures	AC-1.1 AC-1.2	AC-1.1 AC-1.2 AC-1.3 AC-1.4	AC-1.1 AC-1.2 AC-1.3 AC-1.4 AC-1.5 AC-1.6 AC-1.7
AC-2	Account Management	AC-2.1 AC-2.2	AC-2.1 AC-2.2 AC-2.3 AC-2.4 AC-2.5 AC-2.6	AC-2.1 AC-2.2 AC-2.3 AC-2.4 AC-2.5 AC-2.6 AC-2.7 AC-2.8
	Enhancement #1	Not Applicable	AC-2.9	AC-2.9 AC-2.10
	Enhancement #2	Not Applicable	AC-2.11 AC-2.12	AC-2.11 AC-2.12 AC-2.13 AC-2.14
	Enhancement #3	Not Applicable	AC-2.15 AC-2.16	AC-2.15 AC-2.16 AC-2.17 AC-2.18
	Enhancement #4	Not Applicable	Not Applicable	AC-2.19 AC-2.20
AC-3	Access Enforcement	AC-3.1 AC-3.2	AC-3.1 AC-3.2 AC-3.3 AC-3.4	AC-3.1 AC-3.2 AC-3.3 AC-3.4 AC-3.5 AC-3.6
	Enhancement #1	Not Applicable	AC-3.7 AC-3.8	AC-3.7 AC-3.8 AC-3.9
AC-4	Information Flow Enforcement	Not Applicable	AC-4.1 AC-4.2 AC-4.3	AC-4.1 AC-4.2 AC-4.3 AC-4.4 AC-4.5
AC-5	Separation of Duties	Not Applicable	AC-5.1 AC-5.2 AC-5.3	AC-5.1 AC-5.2 AC-5.3 AC-5.4 AC-5.5
AC-6	Least Privilege	Not Applicable	AC-6.1 AC-6.2 AC-6.3 AC-6.4	AC-6.1 AC-6.2 AC-6.3 AC-6.4 AC-6.5 AC-6.6

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
AC-7	Unsuccessful Login Attempts	AC-7.1 AC-7.2	AC-7.1 AC-7.2 AC-7.3 AC-7.4	AC-7.1 AC-7.2 AC-7.3 AC-7.4 AC-7.5 AC-7.6 AC-7.7
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
AC-8	System Use Notification	AC-8.1	AC-8.1 AC-8.2 AC-8.3	AC-8.1 AC-8.2 AC-8.3 AC-8.4 AC-8.5 AC-8.6
AC-9	Previous Logon Notification	Not Applicable	Not Applicable	Not Applicable
AC-10	Concurrent Session Control	Not Applicable	Not Applicable	AC-10.1 AC-10.2 AC-10.3 AC-10.4 AC-10.5
AC-11	Session Lock	Not Applicable	AC-11.1 AC-11.2	AC-11.1 AC-11.2 AC-11.3 AC-11.4 AC-11.5
AC-12	Session Termination	Not Applicable	AC-12.1 AC-12.2	AC-12.1 AC-12.2 AC-12.3 AC-12.4 AC-12.5
AC-13	Supervision and Review—Access Control	AC-13.1 AC-13.2	AC-13.1 AC-13.2 AC-13.3 AC-13.4	AC-13.1 AC-13.2 AC-13.3 AC-13.4 AC-13.5 AC-13.6
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
AC-14	Permitted Actions without Identification or Authentication	AC-14.1 AC-14.2	AC-14.1 AC-14.2 AC-14.3 AC-14.4	AC-14.1 AC-14.2 AC-14.3 AC-14.4 AC-14.5 AC-14.6 AC-14.7
	Enhancement #1	Not Applicable	AC-14.8 AC-14.9	AC-14.8 AC-14.9 AC-14.10
AC-15	Automated Marking	Not Applicable	Not Applicable	AC-15.1 AC-15.2 AC-15.3 AC-15.4 AC-15.5 AC-15.6
AC-16	Automated Labeling	Not Applicable	Not Applicable	Not Applicable

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
AC-17	Remote Access	AC-17.1	AC-17.1 AC-17.2 AC-17.3 AC-17.4 AC-17.5 AC-17.6 AC-17.7	AC-17.1 AC-17.2 AC-17.3 AC-17.4 AC-17.5 AC-17.6 AC-17.7 AC-17.8 AC-17.9
	Enhancement #1	Not Applicable	AC-17.10 AC-17.11	AC-17.12
	Enhancement #2	Not Applicable	AC-17.13	AC-17.14
	Enhancement #3	Not Applicable	AC-17.15	AC-17.16
AC-18	Wireless Access Restrictions	AC-18.1	AC-18.1 AC-18.2 AC-18.3 AC-18.4 AC-18.5	AC-18.1 AC-18.2 AC-18.3 AC-18.4 AC-18.5 AC-18.6 AC-18.7 AC-18.8
	Enhancement #1	Not Applicable	AC-18.9	AC-18.9 AC-18.10
AC-19	Access Control for Portable and Mobile Systems	Not Applicable	AC-19.1 AC-19.2 AC-19.3	AC-19.1 AC-19.2 AC-19.3 AC-19.4 AC-19.5 AC-19.6
	Enhancement #1	Not Applicable	AC-19.7	AC-19.7 AC-19.8 AC-19.9
AC-20	Personally Owned Information Systems	AC-20.1 AC-20.2	AC-20.1 AC-20.2 AC-20.3	AC-20.1 AC-20.2 AC-20.3 AC-20.4 AC-20.5
Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	AT-1.1 AT-1.2	AT-1.1 AT-1.2 AT-1.3 AT-1.4	AT-1.1 AT-1.2 AT-1.3 AT-1.4 AT-1.5 AT-1.6 AT-1.7
AT-2	Security Awareness	AT-2.1	AT-2.1 AT-2.2 AT-2.3	AT-2.1 AT-2.2 AT-2.3 AT-2.4 AT-2.5
AT-3	Security Training	AT-3.1 AT-3.2	AT-3.1 AT-3.2 AT-3.3 AT-3.4	AT-3.1 AT-3.2 AT-3.3 AT-3.4 AT-3.5 AT-3.6

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
AT-4	Security Training Records	AT-4.1	AT-4.1 AT-4.2	AT-4.1 AT-4.2 AT-4.3 AT-4.4
AT-5	Contacts with Security Groups and Associations	Not Applicable	Not Applicable	Not Applicable
Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	AU-1.1 AU-1.2	AU-1.1 AU-1.2 AU-1.3 AU-1.4	AU-1.1 AU-1.2 AU-1.3 AU-1.4 AU-1.5 AU-1.6 AU-1.7
AU-2	Auditable Events	AU-2.1	AU-2.1 AU-2.2 AU-2.3	AU-2.1 AU-2.2 AU-2.3 AU-2.4 AU-2.5
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
	Enhancement #2	Not Applicable	Not Applicable	Not Applicable
AU-3	Content of Audit Records	AU-3.1	AU-3.1 AU-3.2 AU-3.3	AU-3.1 AU-3.2 AU-3.3 AU-3.4 AU-3.5
	Enhancement #1	Not Applicable	AU-3.6 AU-3.7	AU-3.6 AU-3.7
	Enhancement #2	Not Applicable	Not Applicable	AU-3.8 AU-3.9
AU-4	Audit Storage Capacity	AU-4.1	AU-4.1 AU-4.2 AU-4.3	AU-4.1 AU-4.2 AU-4.3 AU-4.4 AU-4.5
AU-5	Audit Processing	AU-5.1	AU-5.1 AU-5.2 AU-5.3	AU-5.1 AU-5.2 AU-5.3 AU-5.4 AU-5.5
	Enhancement #1	Not Applicable	Not Applicable	AU-5.6 AU-5.7
AU-6	Audit Monitoring, Analysis, and Reporting	Not Applicable	AU-6.1 AU-6.2 AU-6.3	AU-6.1 AU-6.2 AU-6.3 AU-6.4 AU-6.5
	Enhancement #1	Not Applicable	Not Applicable	AU-6.6 AU-6.7
	Enhancement #2	Not Applicable	Not Applicable	Not Applicable
AU-7	Audit Reduction and Report Generation	Not Applicable	AU-7.1 AU-7.2 AU-7.3	AU-7.1 AU-7.2 AU-7.3 AU-7.4 AU-7.5

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
	Enhancement #1	Not Applicable	Not Applicable	AU-7.6 AU-7.7
AU-8	Time Stamps	Not Applicable	AU-8.1 AU-8.2 AU-8.3	AU-8.1 AU-8.2 AU-8.3 AU-8.4 AU-8.5
AU-9	Protection of Audit Information	AU-9.1	AU-9.1 AU-9.2 AU-9.3	AU-9.1 AU-9.2 AU-9.3 AU-9.4 AU-9.5
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
AU-10	Non-repudiation	Not Applicable	Not Applicable	Not Applicable
AU-11	Audit Retention	AU-11.1	AU-11.1 AU-11.2	AU-11.1 AU-11.2 AU-11.3 AU-11.4
Certification, Accreditation, and Security Assessments				
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1.1 CA-1.2	CA-1.1 CA-1.2 CA-1.3 CA-1.4	CA-1.1 CA-1.2 CA-1.3 CA-1.4 CA-1.5 CA-1.6 CA-1.7
CA-2	Security Assessments	Not Applicable	CA-2.1 CA-2.2	CA-2.1 CA-2.2 CA-2.3 CA-2.4
CA-3	Information System Connections	CA-3.1 CA-3.2	CA-3.1 CA-3.2 CA-3.3	CA-3.1 CA-3.2 CA-3.3 CA-3.4 CA-3.5
CA-4	Security Certification	CA-4.1 CA-4.2	CA-4.1 CA-4.2 CA-4.3	CA-4.1 CA-4.2 CA-4.3 CA-4.4 CA-4.5
	Enhancement #1	Not Applicable	CA-4.6	CA-4.6
CA-5	Plan of Action and Milestones	CA-5.1 CA-5.2	CA-5.1 CA-5.2 CA-5.3 CA-5.4	CA-5.1 CA-5.2 CA-5.3 CA-5.4 CA-5.5 CA-5.6
CA-6	Security Accreditation	CA-6.1 CA-6.2 CA-6.3	CA-6.1 CA-6.2 CA-6.3 CA-6.4	CA-6.1 CA-6.2 CA-6.3 CA-6.4 CA-6.5 CA-6.6

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
CA-7	Continuous Monitoring	CA-7.1 CA-7.2	CA-7.1 CA-7.2 CA-7.3 CA-7.4	CA-7.1 CA-7.2 CA-7.3 CA-7.4 CA-7.5 CA-7.6
Configuration Management				
CM-1	Configuration Management Policy and Procedures	CM-1.1 CM-1.2	CM-1.1 CM-1.2 CM-1.3 CM-1.4	CM-1.1 CM-1.2 CM-1.3 CM-1.4 CM-1.5 CM-1.6 CM-1.7
CM-2	Baseline Configuration and System Component Inventory	CM-2.1 CM-2.2	CM-2.1 CM-2.2 CM-2.3 CM-2.4 CM-2.5	CM-2.1 CM-2.2 CM-2.3 CM-2.4 CM-2.5 CM-2.6 CM-2.7
	Enhancement #1	Not Applicable	CM-2.8	CM-2.8
	Enhancement #2	Not Applicable	Not Applicable	CM-2.9 CM-2.10 CM-2.11
CM-3	Configuration Change Control	Not Applicable	CM-3.1 CM-3.2 CM-3.3	CM-3.1 CM-3.2 CM-3.3 CM-3.4 CM-3.5
	Enhancement #1	Not Applicable	Not Applicable	CM-3.6 CM-3.7
CM-4	Monitoring Configuration Changes	Not Applicable	CM-4.1 CM-4.2 CM-4.3	CM-4.1 CM-4.2 CM-4.3 CM-4.4 CM-4.5
CM-5	Access Restrictions for Change	Not Applicable	CM-5.1 CM-5.2 CM-5.3 CM-5.4	CM-5.1 CM-5.2 CM-5.3 CM-5.4 CM-5.5 CM-5.6
	Enhancement #1	Not Applicable	Not Applicable	CM-5.7 CM-5.8 CM-5.9
CM-6	Configuration Settings	CM-6.1	CM-6.1 CM-6.2 CM-6.3	CM-6.1 CM-6.2 CM-6.3 CM-6.4 CM-6.5
	Enhancement #1	Not Applicable	Not Applicable	CM-6.6 CM-6.7 CM-6.8

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
CM-7	Least Functionality	Not Applicable	CM-7.1 CM-7.2 CM-7.3	CM-7.1 CM-7.2 CM-7.3 CM-7.4 CM-7.5
	Enhancement #1	Not Applicable	Not Applicable	CM-7.6
Contingency Planning				
CP-1	Contingency Planning Policy and Procedures	CP-1.1 CP-1.2	CP-1.1 CP-1.2 CP-1.3 CP-1.4	CP-1.1 CP-1.2 CP-1.3 CP-1.4 CP-1.5 CP-1.6 CP-1.7
CP-2	Contingency Plan	CP-2.1 CP-2.2	CP-2.1 CP-2.2 CP-2.3 CP-2.4	CP-2.1 CP-2.2 CP-2.3 CP-2.4 CP-2.5 CP-2.6
	Enhancement #1	Not Applicable	CP-2.7	CP-2.7
CP-3	Contingency Training	Not Applicable	CP-3.1 CP-3.2 CP-3.3 CP-3.4	CP-3.1 CP-3.2 CP-3.3 CP-3.4 CP-3.5 CP-3.6
	Enhancement #1	Not Applicable	Not Applicable	CP-3.7 CP-3.8 CP-3.9
	Enhancement #2	Not Applicable	Not Applicable	Not Applicable
CP-4	Contingency Plan Testing	Not Applicable	CP-4.1 CP-4.2 CP-4.3 CP-4.4	CP-4.1 CP-4.2 CP-4.3 CP-4.4 CP-4.5 CP-4.6 CP-4.7
	Enhancement #1	Not Applicable	CP-4.8	CP-4.8
	Enhancement #2	Not Applicable	Not Applicable	CP-4.9
	Enhancement #3	Not Applicable	Not Applicable	Not Applicable
CP-5	Contingency Plan Update	CP-5.1	CP-5.1 CP-5.2 CP-5.3	CP-5.1 CP-5.2 CP-5.3 CP-5.4 CP-5.5
CP-6	Alternate Storage Sites	Not Applicable	CP-6.1 CP-6.2	CP-6.1 CP-6.2 CP-6.3 CP-6.4 CP-6.5
	Enhancement #1	Not Applicable	CP-6.6 CP-6.7	CP-6.6 CP-6.7
	Enhancement #2	Not Applicable	Not Applicable	CP-6.8 CP-6.9

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
	Enhancement #3	Not Applicable	Not Applicable	CP-6.10
CP-7	Alternate Processing Sites	Not Applicable	CP-7.1 CP-7.2	CP-7.1 CP-7.2 CP-7.3 CP-7.4 CP-7.5
	Enhancement #1	Not Applicable	CP-7.6 CP-7.7	CP-7.6 CP-7.7
	Enhancement #2	Not Applicable	CP-7.8	CP-7.8
	Enhancement #3	Not Applicable	CP-7.9	CP-7.9
	Enhancement #4	Not Applicable	Not Applicable	CP-7.10 CP-7.11
CP-8	Telecommunications Services	Not Applicable	CP-8.1 CP-8.2	CP-8.1 CP-8.2 CP-8.3 CP-8.4
	Enhancement #1	Not Applicable	CP-8.5	CP-8.5
	Enhancement #2	Not Applicable	CP-8.6	CP-8.6
	Enhancement #3	Not Applicable	Not Applicable	CP-8.7
	Enhancement #4	Not Applicable	Not Applicable	CP-8.8
CP-9	Information System Backup	CP-9.1 CP-9.2	CP-9.1 CP-9.2 CP-9.3	CP-9.1 CP-9.2 CP-9.3 CP-9.4 CP-9.5
	Enhancement #1	Not Applicable	CP-9.6	CP-9.6
	Enhancement #2	Not Applicable	Not Applicable	CP-9.7
	Enhancement #3	Not Applicable	Not Applicable	CP-9.8
	Enhancement #4	Not Applicable	Not Applicable	Not Applicable
CP-10	Information System Recovery and Reconstitution	CP-10.1	CP-10.1 CP-10.2 CP-10.3 CP-10.4	CP-10.1 CP-10.2 CP-10.3 CP-10.4 CP-10.5 CP-10.6 CP-10.7
	Enhancement #1	Not Applicable	Not Applicable	CP-10.8
Identification and Authentication				
IA-1	Identification and Authentication Policy and Procedures	IA-1.1 IA-1.2	IA-1.1 IA-1.2 IA-1.3 IA-1.4	IA-1.1 IA-1.2 IA-1.3 IA-1.4 IA-1.5 IA-1.6 IA-1.7

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
IA-2	User Identification and Authentication	IA-2.1 IA-2.2	IA-2.1 IA-2.2 IA-2.3 IA-2.4	IA-2.1 IA-2.2 IA-2.3 IA-2.4 IA-2.5 IA-2.6 IA-2.7 IA-2.8
	Enhancement #1	Not Applicable	Not Applicable	IA-2.9 IA-2.10
IA-3	Device Identification and Authentication	Not Applicable	IA-3.1 IA-3.2 IA-3.3	IA-3.1 IA-3.2 IA-3.3 IA-3.4 IA-3.5 IA-3.6
IA-4	Identifier Management	IA-4.1	IA-4.1 IA-4.2 IA-4.3	IA-4.1 IA-4.2 IA-4.3 IA-4.4 IA-4.5
IA-5	Authenticator Management	IA-5.1 IA-5.2 IA-5.3	IA-5.1 IA-5.2 IA-5.3 IA-5.4 IA-5.5 IA-5.6	IA-5.1 IA-5.2 IA-5.3 IA-5.4 IA-5.5 IA-5.6 IA-5.7 IA-5.8 IA-5.9
IA-6	Authenticator Feedback	IA-6.1	IA-6.1 IA-6.2 IA-6.3	IA-6.1 IA-6.2 IA-6.3 IA-6.4 IA-6.5
IA-7	Cryptographic Module Authentication	IA-7.1 IA-7.2 IA-7.3	IA-7.1 IA-7.2 IA-7.3 IA-7.4	IA-7.1 IA-7.2 IA-7.3 IA-7.4 IA-7.5 IA-7.6
Incident Response				
IR-1	Incident Response Policy and Procedures	IR-1.1 IR-1.2	IR-1.1 IR-1.2 IR-1.3 IR-1.4	IR-1.1 IR-1.2 IR-1.3 IR-1.4 IR-1.5 IR-1.6 IR-1.7
IR-2	Incident Response Training	Not Applicable	IR-2.1 IR-2.2 IR-2.3 IR-2.4	IR-2.1 IR-2.2 IR-2.3 IR-2.4 IR-2.5 IR-2.6
	Enhancement #1	Not Applicable	Not Applicable	IR-2.7 IR-2.8 IR-2.9

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
	Enhancement #2	Not Applicable	Not Applicable	Not Applicable
IR-3	Incident Response Testing	Not Applicable	IR-3.1 IR-3.2 IR-3.3 IR-3.4	IR-3.1 IR-3.2 IR-3.3 IR-3.4 IR-3.5 IR-3.6
	Enhancement #1	Not Applicable	Not Applicable	IR-3.7 IR-3.8 IR-3.9
IR-4	Incident Handling	IR-4.1	IR-4.1 IR-4.2 IR-4.3	IR-4.1 IR-4.2 IR-4.3 IR-4.4 IR-4.5
	Enhancement #1	Not Applicable	IR-4.6	IR-4.6 IR-4.7 IR-4.8
IR-5	Incident Monitoring	Not Applicable	IR-5.1 IR-5.2 IR-5.3	IR-5.1 IR-5.2 IR-5.3 IR-5.4 IR-5.5
	Enhancement #1	Not Applicable	Not Applicable	IR-5.6 IR-5.7 IR-5.8
IR-6	Incident Reporting	IR-6.1	IR-6.1 IR-6.2 IR-6.3	IR-6.1 IR-6.2 IR-6.3 IR-6.4 IR-6.5
	Enhancement #1	Not Applicable	IR-6.6	IR-6.6 IR-6.7 IR-6.8
IR-7	Incident Response Assistance	IR-7.1	IR-7.1 IR-7.2 IR-7.3	IR-7.1 IR-7.2 IR-7.3 IR-7.4 IR-7.5
	Enhancement #1	Not Applicable	IR-7.6	IR-7.6 IR-7.7 IR-7.8
Maintenance				
MA-1	System Maintenance Policy and Procedures	MA-1.1 MA-1.2	MA-1.1 MA-1.2 MA-1.3 MA-1.4	MA-1.1 MA-1.2 MA-1.3 MA-1.4 MA-1.5 MA-1.6 MA-1.7
MA-2	Periodic Maintenance	MA-2.1 MA-2.2	MA-2.1 MA-2.2 MA-2.3	MA-2.1 MA-2.2 MA-2.3 MA-2.4 MA-2.5
	Enhancement #1	Not Applicable	MA-2.6	MA-2.6

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
	Enhancement #2	Not Applicable	Not Applicable	MA-2.7 MA-2.8
MA-3	Maintenance Tools	Not Applicable	MA-3.1 MA-3.2 MA-3.3	MA-3.1 MA-3.2 MA-3.3 MA-3.4 MA-3.5
	Enhancement #1	Not Applicable	Not Applicable	MA-3.6 MA-3.7
	Enhancement #2	Not Applicable	Not Applicable	MA-3.8 MA-3.9
	Enhancement #3	Not Applicable	Not Applicable	MA-3.10 MA-3.11 MA-3.12
	Enhancement #4	Not Applicable	Not Applicable	Not Applicable
MA-4	Remote Maintenance	MA-4.1	MA-4.1 MA-4.2	MA-4.1 MA-4.2 MA-4.3 MA-4.4
	Enhancement #1	Not Applicable	Not Applicable	MA-4.5
	Enhancement #2	Not Applicable	Not Applicable	MA-4.6
	Enhancement #3	Not Applicable	Not Applicable	MA-4.7
MA-5	Maintenance Personnel	MA-5.1	MA-5.1 MA-5.2	MA-5.1 MA-5.2 MA-5.3 MA-5.4
MA-6	Timely Maintenance	Not Applicable	MA-6.1 MA-6.2	MA-6.1 MA-6.2 MA-6.3 MA-6.4
Media Protection				
MP-1	Media Protection Policy and Procedures	MP-1.1 MP-1.2	MP-1.1 MP-1.2 MP-1.3 MP-1.4	MP-1.1 MP-1.2 MP-1.3 MP-1.4 MP-1.5 MP-1.6 MP-1.7
MP-2	Media Access	MP-2.1	MP-2.1 MP-2.2	MP-2.1 MP-2.2 MP-2.3 MP-2.4
	Enhancement #1	Not Applicable	Not Applicable	MP-2.5 MP-2.6 MP-2.7
MP-3	Media Labeling	Not Applicable	MP-3.1 MP-3.2 MP-3.3 MP-3.4	MP-3.1 MP-3.2 MP-3.3 MP-3.4 MP-3.5 MP-3.6

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
MP-4	Media Storage	Not Applicable	MP-4.1 MP-4.2 MP-4.3	MP-4.1 MP-4.2 MP-4.3 MP-4.4 MP-4.5
MP-5	Media Transport	Not Applicable	MP-5.1 MP-5.2 MP-5.3	MP-5.1 MP-5.2 MP-5.3 MP-5.4 MP-5.5
MP-6	Media Sanitization and Disposal	MP-6.1 MP-6.2	MP-6.1 MP-6.2 MP-6.3	MP-6.1 MP-6.2 MP-6.3 MP-6.4 MP-6.5
Physical and Environmental Protection				
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1.1 PE-1.2	PE-1.1 PE-1.2 PE-1.3 PE-1.4	PE-1.1 PE-1.2 PE-1.3 PE-1.4 PE-1.5 PE-1.6 PE-1.7
PE-2	Physical Access Authorizations	PE-2.1	PE-2.1 PE-2.2 PE-2.3	PE-2.1 PE-2.2 PE-2.3 PE-2.4 PE-2.5
PE-3	Physical Access Control	PE-3.1	PE-3.1 PE-3.2 PE-3.3 PE-3.4	PE-3.1 PE-3.2 PE-3.3 PE-3.4 PE-3.5 PE-3.6
PE-4	Access Control for Transmission Medium	Not Applicable	Not Applicable	PE-4.1 PE-4.2 PE-4.3 PE-4.4
PE-5	Access Control for Display Medium	Not Applicable	PE-5.1 PE-5.2	PE-5.1 PE-5.2 PE-5.3 PE-5.4
PE-6	Monitoring Physical Access	PE-6.1	PE-6.1 PE-6.2 PE-6.3	PE-6.1 PE-6.2 PE-6.3 PE-6.4 PE-6.5
	Enhancement #1	Not Applicable	PE-6.6 PE-6.7	PE-6.6 PE-6.7
	Enhancement #2	Not Applicable	Not Applicable	PE-6.8 PE-6.9 PE-6.10
PE-7	Visitor Control	PE-7.1	PE-7.1 PE-7.2 PE-7.3	PE-7.1 PE-7.2 PE-7.3 PE-7.4 PE-7.5

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
	Enhancement #1	Not Applicable	PE-7.6	PE-7.6
PE-8	Access Logs	PE-8.1	PE-8.1 PE-8.2	PE-8.1 PE-8.2 PE-8.3 PE-8.4
	Enhancement #1	Not Applicable	Not Applicable	PE-8.5 PE-8.6
PE-9	Power Equipment and Power Cabling	Not Applicable	PE-9.1 PE-9.2	PE-9.1 PE-9.2 PE-9.3 PE-9.4
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
PE-10	Emergency Shutoff	Not Applicable	PE-10.1 PE-10.2 PE-10.3	PE-10.1 PE-10.2 PE-10.3 PE-10.4 PE-10.5
PE-11	Emergency Power	Not Applicable	PE-11.1 PE-11.2 PE-11.3	PE-11.1 PE-11.2 PE-11.3 PE-11.4 PE-11.5
	Enhancement #1	Not Applicable	Not Applicable	PE-11.6 PE-11.7
	Enhancement #2	Not Applicable	Not Applicable	Not Applicable
PE-12	Emergency Lighting	PE-12.1	PE-12.1 PE-12.2 PE-12.3	PE-12.1 PE-12.2 PE-12.3 PE-12.4 PE-12.5
PE-13	Fire Protection	PE-13.1	PE-13.1 PE-13.2 PE-13.3	PE-13.1 PE-13.2 PE-13.3 PE-13.4 PE-13.5
	Enhancement #1	Not Applicable	PE-13.6	PE-13.6
	Enhancement #2	Not Applicable	Not Applicable	PE-13.7 PE-13.8 PE-13.9
PE-14	Temperature and Humidity Controls	PE-14.1 PE-14.2	PE-14.1 PE-14.2 PE-14.3	PE-14.1 PE-14.2 PE-14.3 PE-14.4 PE-14.5
PE-15	Water Damage Protection	PE-15.1 PE-15.2	PE-15.1 PE-15.2 PE-15.3 PE-15.4	PE-15.1 PE-15.2 PE-15.3 PE-15.4 PE-15.5 PE-15.6
	Enhancement #1	Not Applicable	Not Applicable	PE-15.7 PE-15.8

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
PE-16	Delivery and Removal	PE-16.1	PE-16.1 PE-16.2	PE-16.1 PE-16.2 PE-16.3 PE-16.4
PE-17	Alternate Work Site	Not Applicable	PE-17.1 PE-17.2	PE-17.1 PE-17.2 PE-17.3 PE-17.4 PE-17.5
PE-18	Location of Information System Components	Not Applicable	PE-18.1 PE-18.2 PE-18.3	PE-18.1 PE-18.2 PE-18.3 PE-18.4 PE-18.5
PE-19	Information Leakage	Not Applicable	Not Applicable	Not Applicable
Planning				
PL-1	Security Planning Policy and Procedures	PL-1.1 PL-1.2	PL-1.1 PL-1.2 PL-1.3 PL-1.4	PL-1.1 PL-1.2 PL-1.3 PL-1.4 PL-1.5 PL-1.6 PL-1.7
PL-2	System Security Plan	PL-2.1 PL-2.2	PL-2.1 PL-2.2 PL-2.3 PL-2.4	PL-2.1 PL-2.2 PL-2.3 PL-2.4 PL-2.5 PL-2.6
PL-3	System Security Plan Update	PL-3.1	PL-3.1 PL-3.2 PL-3.3	PL-3.1 PL-3.2 PL-3.3 PL-3.4 PL-3.5
PL-4	Rules of Behavior	PL-4.1 PL-4.2 PL-4.3	PL-4.1 PL-4.2 PL-4.3 PL-4.4 PL-4.5	PL-4.1 PL-4.2 PL-4.3 PL-4.4 PL-4.5 PL-4.6 PL-4.7
PL-5	Privacy Impact Assessment	PL-5.1	PL-5.1 PL-5.2	PL-5.1 PL-5.2 PL-5.3 PL-5.4
PL-6	Security-Related Activity Planning	Not Applicable	PL-6.1 PL-6.2 PL-6.3	PL-6.1 PL-6.2 PL-6.3 PL-6.4 PL-6.5

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
Personnel Security				
PS-1	Personnel Security Policy and Procedures	PS-1.1 PS-1.2	PS-1.1 PS-1.2 PS-1.3 PS-1.4	PS-1.1 PS-1.2 PS-1.3 PS-1.4 PS-1.5 PS-1.6 PS-1.7
PS-2	Position Categorization	PS-2.1	PS-2.1 PS-2.2 PS-2.3	PS-2.1 PS-2.2 PS-2.3 PS-2.4 PS-2.5
PS-3	Personnel Screening	PS-3.1	PS-3.1 PS-3.2 PS-3.3	PS-3.1 PS-3.2 PS-3.3 PS-3.4 PS-3.5
PS-4	Personnel Termination	PS-4.1	PS-4.1 PS-4.2	PS-4.1 PS-4.2 PS-4.3 PS-4.4
PS-5	Personnel Transfer	PS-5.1	PS-5.1 PS-5.2 PS-5.3	PS-5.1 PS-5.2 PS-5.3 PS-5.4 PS-5.5
PS-6	Access Agreements	PS-6.1	PS-6.1 PS-6.2 PS-6.3	PS-6.1 PS-6.2 PS-6.3 PS-6.4 PS-6.5
PS-7	Third-Party Personnel Security	PS-7.1	PS-7.1 PS-7.2 PS-7.3 PS-7.4	PS-7.1 PS-7.2 PS-7.3 PS-7.4 PS-7.5 PS-7.6
PS-8	Personnel Sanctions	PS-8.1	PS-8.1 PS-8.2 PS-8.3	PS-8.1 PS-8.2 PS-8.3 PS-8.4 PS-8.5
Risk Assessment				
RA-1	Risk Assessment Policy and Procedures	RA-1.1 RA-1.2	RA-1.1 RA-1.2 RA-1.3 RA-1.4	RA-1.1 RA-1.2 RA-1.3 RA-1.4 RA-1.5 RA-1.6 RA-1.7
RA-2	Security Categorization	RA-2.1 RA-2.2	RA-2.1 RA-2.2 RA-2.3	RA-2.1 RA-2.2 RA-2.3 RA-2.4 RA-2.5

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
RA-3	Risk Assessment	RA-3.1 RA-3.2	RA-3.1 RA-3.2 RA-3.3	RA-3.1 RA-3.2 RA-3.3 RA-3.4 RA-3.5
RA-4	Risk Assessment Update	RA-4.1	RA-4.1 RA-4.2 RA-4.3	RA-4.1 RA-4.2 RA-4.3 RA-4.4 RA-4.5
RA-5	Vulnerability Scanning	Not Applicable	RA-5.1 RA-5.2 RA-5.3 RA-5.4	RA-5.1 RA-5.2 RA-5.3 RA-5.4 RA-5.5 RA-5.6
	Enhancement #1	Not Applicable	Not Applicable	RA-5.7 RA-5.8
	Enhancement #2	Not Applicable	Not Applicable	RA-5.9
	Enhancement #3	Not Applicable	Not Applicable	Not Applicable
System and Services Acquisition				
SA-1	System and Services Acquisition Policy and Procedures	SA-1.1 SA-1.2	SA-1.1 SA-1.2 SA-1.3 SA-1.4	SA-1.1 SA-1.2 SA-1.3 SA-1.4 SA-1.5 SA-1.6 SA-1.7
SA-2	Allocation of Resources	SA-2.1	SA-2.1 SA-2.2	SA-2.1 SA-2.2 SA-2.3 SA-2.4
SA-3	Life Cycle Support	SA-3.1 SA-3.2	SA-3.1 SA-3.2 SA-3.3	SA-3.1 SA-3.2 SA-3.3 SA-3.4 SA-3.5
SA-4	Acquisitions	SA-4.1	SA-4.1 SA-4.2 SA-4.3 SA-4.4	SA-4.1 SA-4.2 SA-4.3 SA-4.4 SA-4.5 SA-4.6 SA-4.7
SA-5	Information System Documentation	SA-5.1	SA-5.1 SA-5.2 SA-5.3	SA-5.1 SA-5.2 SA-5.3 SA-5.4 SA-5.5
	Enhancement #1	Not Applicable	SA-5.6	SA-5.6
	Enhancement #2	Not Applicable	Not Applicable	SA-5.7
SA-6	Software Usage Restrictions	SA-6.1	SA-6.1 SA-6.2	SA-6.1 SA-6.2 SA-6.3 SA-6.4

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
SA-7	User Installed Software	SA-7.1 SA-7.2	SA-7.1 SA-7.2 SA-7.3 SA-7.4 SA-7.5 SA-7.6 SA-7.7	SA-7.1 SA-7.2 SA-7.3 SA-7.4 SA-7.5 SA-7.6 SA-7.7 SA-7.8 SA-7.9
SA-8	Security Design Principles	Not Applicable	SA-8.1 SA-8.2	SA-8.1 SA-8.2 SA-8.3 SA-8.4
SA-9	Outsourced Information System Services	SA-9.1	SA-9.1 SA-9.2 SA-9.3	SA-9.1 SA-9.2 SA-9.3 SA-9.4 SA-9.5 SA-9.6
SA-10	Developer Configuration Management	Not Applicable	Not Applicable	SA-10.1 SA-10.2 SA-10.3 SA-10.4
SA-11	Developer Security Testing	Not Applicable	SA-11.1 SA-11.2 SA-11.3	SA-11.1 SA-11.2 SA-11.3 SA-11.4 SA-11.5
System and Communications Protection				
SC-1	System and Communications Protection Policy and Procedures	SC-1.1 SC-1.2	SC-1.1 SC-1.2 SC-1.3 SC-1.4	SC-1.1 SC-1.2 SC-1.3 SC-1.4 SC-1.5 SC-1.6 SC-1.7
SC-2	Application Partitioning	Not Applicable	SC-2.1 SC-2.2	SC-2.1 SC-2.2 SC-2.3 SC-2.4
SC-3	Security Function Isolation	Not Applicable	Not Applicable	SC-3.1 SC-3.2 SC-3.3 SC-3.4
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
	Enhancement #2	Not Applicable	Not Applicable	Not Applicable
	Enhancement #3	Not Applicable	Not Applicable	Not Applicable
	Enhancement #4	Not Applicable	Not Applicable	Not Applicable
	Enhancement #5	Not Applicable	Not Applicable	Not Applicable
SC-4	Information Remnants	Not Applicable	SC-4.1 SC-4.2	SC-4.1 SC-4.2 SC-4.3 SC-4.4

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
SC-5	Denial of Service Protection	SC-5.1	SC-5.1 SC-5.2 SC-5.3	SC-5.1 SC-5.2 SC-5.3 SC-5.4 SC-5.5 SC-5.6
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
	Enhancement #2	Not Applicable	Not Applicable	Not Applicable
SC-6	Resource Priority	Not Applicable	Not Applicable	Not Applicable
SC-7	Boundary Protection	SC-7.1	SC-7.1 SC-7.2	SC-7.1 SC-7.2 SC-7.3 SC-7.4
	Enhancement #1	Not Applicable	SC-7.5	SC-7.5
SC-8	Transmission Integrity	Not Applicable	SC-8.1 SC-8.2	SC-8.1 SC-8.2 SC-8.3 SC-8.4
	Enhancement #1	Not Applicable	Not Applicable	SC-8.5 SC-8.6 SC-8.7
SC-9	Transmission Confidentiality	Not Applicable	SC-9.1 SC-9.2	SC-9.1 SC-9.2 SC-9.3 SC-9.4
	Enhancement #1	Not Applicable	Not Applicable	SC-9.5 SC-9.6 SC-9.7
SC-10	Network Disconnect	Not Applicable	SC-10.1 SC-10.2 SC-10.3	SC-10.1 SC-10.2 SC-10.3 SC-10.4 SC-10.5
SC-11	Trusted Path	Not Applicable	Not Applicable	Not Applicable
SC-12	Cryptographic Key Establishment and Mgmt.		SC-12.1 SC-12.2 SC-12.3	SC-12.1 SC-12.2 SC-12.3 SC-12.4 SC-12.5
SC-13	Use of Validated Cryptography	SC-13.1	SC-13.1 SC-13.2	SC-13.1 SC-13.2 SC-13.3
SC-14	Public Access Protections	SC-14.1	SC-14.1 SC-14.2 SC-14.3	SC-14.1 SC-14.2 SC-14.3 SC-14.4 SC-14.5
SC-15	Collaborative Computing	Not Applicable	SC-15.1 SC-15.2 SC-15.3	SC-15.1 SC-15.2 SC-15.3 SC-15.4 SC-15.5
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
SC-16	Transmission of Security Parameters	Not Applicable	Not Applicable	Not Applicable

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
SC-17	Public Key Infrastructure Certificates	Not Applicable	SC-17.1 SC-17.2	SC-17.1 SC-17.2 SC-17.3 SC-17.4
SC-18	Mobile Code	Not Applicable	SC-18.1 SC-18.2 SC-18.3	SC-18.1 SC-18.2 SC-18.3 SC-18.4 SC-18.5
SC-19	Voice Over Internet Protocol	Not Applicable	SC-19.1 SC-19.2 SC-19.3 SC-19.4	SC-19.1 SC-19.2 SC-19.3 SC-19.4 SC-19.5 SC-19.6
SC-20	Secure Name Lookup Service (Authoritative Source)	Not Applicable	SC-20.1 SC-20.2 SC-20.3	SC-20.1 SC-20.2 SC-20.3 SC-20.4 SC-20.5
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
SC-21	Secure Name Lookup Service (Resolution)	Not Applicable	Not Applicable	SC-21.1 SC-21.2 SC-21.3 SC-21.4 SC-21.5
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
System and Information Integrity				
SI-1	System and Information Integrity Policy and Procedures	SI-1.1 SI-1.2	SI-1.1 SI-1.2 SI-1.3 SI-1.4	SI-1.1 SI-1.2 SI-1.3 SI-1.4 SI-1.5 SI-1.6 SI-1.7
SI-2	Flaw Remediation	SI-2.1 SI-2.2	SI-2.1 SI-2.2 SI-2.3 SI-2.4 SI-2.5	SI-2.1 SI-2.2 SI-2.3 SI-2.4 SI-2.5 SI-2.6 SI-2.7 SI-2.8 SI-2.9 SI-2.10 SI-2.11
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
	Enhancement #2	Not Applicable	Not Applicable	Not Applicable

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
SI-3	Malicious Code Protection	SI-3.1	SI-3.1 SI-3.2 SI-3.3 SI-3.4 SI-3.5	SI-3.1 SI-3.2 SI-3.3 SI-3.4 SI-3.5 SI-3.6 SI-3.7 SI-3.8 SI-3.9
	Enhancement #1	Not Applicable	SI-3.10	SI-3.10
	Enhancement #2	Not Applicable	Not Applicable	SI-3.11
SI-4	Information System Monitoring Tools and Techniques		SI-4.1 SI-4.2 SI-4.3 SI-4.4	SI-4.1 SI-4.2 SI-4.3 SI-4.4 SI-4.5 SI-4.6
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
	Enhancement #2	Not Applicable	Not Applicable	Not Applicable
	Enhancement #3	Not Applicable	Not Applicable	Not Applicable
	Enhancement #4	Not Applicable	Not Applicable	Not Applicable
SI-5	Security Alerts and Advisories	SI-5.1	SI-5.1 SI-5.2 SI-5.3	SI-5.1 SI-5.2 SI-5.3 SI-5.4 SI-5.5
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
SI-6	Security Functionality Verification	Not Applicable	Not Applicable	SI-6.1 SI-6.2 SI-6.3 SI-6.4 SI-6.5 SI-6.6
	Enhancement #1	Not Applicable	Not Applicable	Not Applicable
	Enhancement #2	Not Applicable	Not Applicable	Not Applicable
SI-7	Software and Information Integrity	Not Applicable	Not Applicable	SI-7.1 SI-7.2 SI-7.3 SI-7.4 SI-7.5 SI-7.6 SI-7.7
SI-8	Spam Protection	Not Applicable	SI-8.1 SI-8.2 SI-8.3 SI-8.4	SI-8.1 SI-8.2 SI-8.3 SI-8.4 SI-8.5 SI-8.6 SI-8.7
	Enhancement #1	Not Applicable	Not Applicable	SI-8.8
	Enhancement #2	Not Applicable	Not Applicable	Not Applicable

CNTL NO.	CONTROL NAME	MINIMUM ASSESSMENT PROCEDURES		
		LOW Baseline	MODERATE Baseline	HIGH Baseline
SI-9	Information Input Restrictions	Not Applicable	SI-9.1 SI-9.2 SI-9.3	SI-9.1 SI-9.2 SI-9.3 SI-9.4 SI-9.5
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	Not Applicable	SI-10.1 SI-10.2 SI-10.3 SI-10.4	SI-10.1 SI-10.2 SI-10.3 SI-10.4 SI-10.5 SI-10.6
SI-11	Error Handling	Not Applicable	SI-11.1 SI-11.2 SI-11.3 SI-11.4 SI-11.5 SI-11.6	SI-11.1 SI-11.2 SI-11.3 SI-11.4 SI-11.5 SI-11.6 SI-11.7 SI-11.8
SI-12	Information Output Handling and Retention	Not Applicable	SI-12.1 SI-12.2 SI-12.3	SI-12.1 SI-12.2 SI-12.3 SI-12.4 SI-12.5