NIST Special Publication 800-171A

Assessing Security Requirements for Controlled Unclassified Information

RON ROSS
KELLEY DEMPSEY
VICTORIA PILLITTERI

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-171A

Assessing Security Requirements for Controlled Unclassified Information

RON ROSS
KELLEY DEMPSEY
VICTORIA PILLITTERI
Computer Security Division
National Institute of Standards and Technology

June 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by the National Institute of Standards and Technology to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the 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 OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-171A
Natl. Inst. Stand. Technol. Spec. Publ. 800-171A, **92 pages** (June 2018)

CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171A

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

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts, practices, and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review draft publications during the designated public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at **https://csrc.nist.gov/publications**.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: **sec-cert@nist.gov**

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The NIST Information Technology Laboratory (ITL) promotes the United States 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 of other than national security-related information and protection of individuals' privacy in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information systems security and its collaborative activities with industry, government, and academic organizations.

Abstract

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its assigned missions and business operations. This publication provides federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements in NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. The assessment procedures are flexible and can be customized to the needs of the organizations and the assessors conducting the assessments. Security assessments can be conducted as self-assessments; independent, third-party assessments; or government-sponsored assessments and can be applied with various degrees of rigor, based on customer-defined depth and coverage attributes. The findings and evidence produced during the security assessments can facilitate risk-based decisions by organizations related to the CUI requirements.

Keywords

Assessment; Assessment Method; Assessment Object; Assessment Procedure; Assurance; Basic Security Requirement; Controlled Unclassified Information; Coverage; CUI Registry; Depth; Derived Security Requirement; Executive Order 13556; FISMA; NIST Special Publication 800-53; NIST Special Publication 800-53A; Nonfederal Organization; Nonfederal System; Security Assessment; Security Control.

Acknowledgements

The authors gratefully acknowledge and appreciate the contributions from Jon Boyens, Devin Casey, Chris Enloe, Ned Goren, Gary Guissanie, Jody Jacobs, Jeff Marron, Vicki Michetti, Mark Riddle, Mary Thomas, Matt Scholl, Gary Stoneburner, Patricia Toth, and Patrick Viscuso whose thoughtful and constructive comments improved the quality, thoroughness, and usefulness of this publication. A special note of thanks goes to Jim Foti and Elizabeth Lennon for their superb administrative and technical editing support.

CAUTIONARY NOTE

The generalized assessment procedures described in this publication provide a framework and a starting point for developing specific procedures to assess the CUI security requirements in NIST Special Publication 800-171. The assessment procedures can be used to generate relevant evidence to determine if the security safeguards employed by organizations are implemented correctly, are operating as intended, and satisfy the CUI security requirements. Organizations have the flexibility to specialize the assessment procedures by selecting the specific assessment methods and the set of assessment objects to achieve the assessment objectives. There is no expectation that all assessment methods and all objects will be used for every assessment. There is also significant flexibility on the scope of the assessment and the degree of rigor applied during the assessment process. The assessment procedures and methods can be applied across a continuum of approaches—including self-assessments; independent, third-party assessments; and assessments conducted by sponsoring organizations (e.g., government agencies). Such approaches may be specified in contracts or in agreements by participating parties.

DEFINITION AND USAGE OF THE TERM INFORMATION SYSTEM

Unless otherwise specified by legislation, regulation, or governmentwide policy, the use of the term *information system* in this publication is replaced by the term *system*. This change reflects a more broad-based and holistic definition of information systems that includes, for example: general purpose information systems; industrial and process control systems; cyber-physical systems; and individual devices that are part of the Internet of Things. As computing platforms and information technologies are increasingly deployed ubiquitously worldwide and systems and components are connected through wired and wireless networks, the susceptibility of Controlled Unclassified Information to loss or compromise grows—as does the potential for adverse consequences resulting from such occurrences.

OTHER RESOURCES TO SUPPORT ASSESSMENTS

NIST Special Publication 800-171A is a companion publication developed to support assessments of the CUI security requirements in NIST Special Publication 800-171. As such, it is the primary and authoritative source of guidance for organizations conducting such assessments. However, since it is recognized that the communities of interest affected by the CUI security requirements are broad and diverse, other supporting assessment guidance may be developed for those communities. For example, the NIST Manufacturing Extension Partnership (MEP) developed Handbook 162, *NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*. This resource, along with other assessment resources that may be developed in the future, can complement the assessment procedures in NIST Special Publication 800-171A, thus helping sector-specific organizations generate the evidence needed to determine if the CUI security requirements have been satisfied.

Table of Contents

Errata

This table contains changes that have been incorporated into Special Publication 800-171A. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature.

DATE	TYPE	REVISION	PAGE

CHAPTER ONE

INTRODUCTION

THE NEED TO ASSESS CUI SECURITY REQUIREMENTS

The protection of unclassified federal information in nonfederal systems and organizations is dependent on the federal government providing a process for identifying the different types of information that are used by federal agencies. Executive Order 13556 established a governmentwide Controlled Unclassified Information (CUI)[1] Program to standardize the way the executive branch handles unclassified information that requires protection. The implementing regulation for the CUI Program is 32 CFR part 2002, *Controlled Unclassified Information*. Only federal information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI.[2] NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, specifies the security requirements to ensure the confidentiality of CUI.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide procedures for assessing the CUI requirements in NIST Special Publication 800-171. Compliance with the security requirements is addressed in CUI guidance and the CUI Federal Acquisition Regulation (FAR)[3] or as supplemented by federal agencies (e.g., Department of Defense Federal Acquisition Regulation). Organizations can use the assessment procedures to generate evidence to support the assertion that the security requirements have been satisfied.

The assessment process is an information-gathering and evidence-producing activity to determine the effectiveness of the safeguards intended to meet the set of security requirements specified in NIST Special Publication 800-171. In this context, the information gathered and the evidence produced can be used by an organization to:

- Identify potential problems or shortfalls in the organization's security and risk management programs;
- Identify security weaknesses and deficiencies in its systems and in the environments in which those systems operate;
- Prioritize risk mitigation decisions and activities;
- Confirm that identified security weaknesses and deficiencies in the system and in the environment of operation have been addressed; and
- Support continuous monitoring activities and provide information security situational awareness.

[1] *Controlled Unclassified Information* is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

[2] The CUI Registry is the online repository for information, guidance, policy, and requirements on handling CUI.

[3] The CUI Executive Agent is actively engaged in the process of developing a FAR clause that will apply the requirements of the federal CUI regulation and NIST Special Publication 800-171 to contractors.

The assessment procedures in this publication offer the flexibility to customize assessments based on organizational policies and requirements, known threat and vulnerability information, system and platform dependencies, operational considerations, and tolerance for risk.[4]

THE SCOPE OF CUI SECURITY REQUIREMENT ASSESSMENTS

For the CUI security requirements in NIST Special Publication 800-171, nonfederal organizations describe in a *system security plan*, how the specified requirements are met or how organizations plan to meet the requirements. The plan describes the system boundary; the environment in which the system operates; how the requirements are implemented; and the relationships with or connections to other systems. The scope of the assessments conducted using the procedures described in this publication are guided and informed by the individual system security plans for the organizational systems processing, storing, or transmitting CUI. The assessments focus on the implementation and effectiveness of the safeguards intended to meet a fixed set of security requirements as defined in NIST Special Publication 800-171.

1.2 TARGET AUDIENCE

This publication serves system, information security, and privacy[5] professionals including individuals with:

- System development responsibilities (e.g., program managers, system developers, system owners, systems integrators, system security engineers);
- Information security assessment and monitoring responsibilities (e.g., system evaluators, assessors, independent verifiers/validators, auditors, analysts, system owners);
- Information security, privacy, risk management, governance, and oversight responsibilities (e.g., authorizing officials, chief information officers, chief privacy officers, chief information security officers, system managers, information security managers); and
- Information security implementation and operational responsibilities (e.g., system owners, information owners/stewards, mission and business owners, systems administrators, system security officers).

1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- Chapter Two describes the fundamental concepts associated with assessments of CUI security requirements including assessment procedures, methods, objects, and assurance cases that can be created using evidence produced during assessments.

[4] The term *risk* is used to mean risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. See NIST Special Publication 800-39 for additional information on organizational risk management and risk tolerance.

[5] References to privacy in this publication are made *only* in the context of where security and privacy considerations overlap—that is, in the security objective of *confidentiality*, which generally supports privacy and the protection of personally identifiable information from unauthorized disclosure. NIST Internal Report 8062 provides additional information on the overlapping and complementary nature of security and privacy disciplines.

- Chapter Three provides a catalog of assessment procedures for the fourteen families of CUI security requirements in NIST Special Publication 800-171, including assessment objectives and potential assessment methods and objects for each procedure.
- Supporting appendices provide additional assessment-related information including general references; definitions and terms; acronyms; and a description of the assessment methods used in assessment procedures.

CHAPTER TWO

THE FUNDAMENTALS

BASIC CONCEPTS FOR ASSESSMENTS OF CUI SECURITY REQUIREMENTS

The CUI security requirements in NIST Special Publication 800-171 are organized into fourteen families. Each family contains the requirements related to the general security topic of the family. Table 1 lists the CUI security requirement families addressed in this publication. The assessment procedures in Chapter Three are grouped by family designations to help ensure completeness and consistency of assessments.

TABLE 1: CUI SECURITY REQUIREMENT FAMILIES

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

2.1 ASSESSMENT PROCEDURES

An assessment procedure consists of an assessment *objective* and a set of potential assessment *methods* and assessment *objects* that can be used to conduct the assessment. Each assessment objective includes a determination statement related to the CUI security requirement that is the subject of the assessment. The determination statements are linked to the content of the CUI security requirements to ensure traceability of the assessment results to the requirements. The application of an assessment procedure to a security requirement produces assessment *findings*. These findings reflect, or are subsequently used, to help determine if the security requirement has been satisfied.

Assessment objects identify the specific items being assessed and can include specifications, mechanisms, activities, and individuals. Specifications are the document-based artifacts (e.g., policies, procedures, security plans, security requirements, functional specifications, architectural designs) associated with a system. Mechanisms are the specific hardware, software, or firmware safeguards employed within a system. Activities are the protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising a contingency plan, and monitoring network traffic). Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above.

The assessment methods define the nature and the extent of the assessor's actions. The methods include *examine*, *interview*, and *test*. The examine method is the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities). The purpose of the examine method is to facilitate understanding, achieve clarification, or obtain evidence. The interview method is the process of holding discussions with individuals or groups

of individuals to facilitate understanding, achieve clarification, or obtain evidence. And finally, the test method is the process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior. In all three assessment methods, the results are used in making specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure.

The assessment methods described above have associated attributes of *depth* and *coverage*, which define the level of effort for the assessment. These attributes provide a means to define the rigor and scope of the assessment for the increased assurance of security requirements. A description of assessment methods and objects is provided in Appendix D.[6] Figure 1 illustrates an example of an assessment procedure for CUI security requirement 3.1.3 from NIST Special Publication 800-171.

3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

FIGURE 1: ASSESSMENT PROCEDURE FOR CUI SECURITY REQUIREMENT

Organizations are not expected to employ *all* assessment methods and objects contained within the assessment procedures identified in this publication. Rather, organizations have the flexibility to determine the level of effort needed and the assurance required for an assessment (e.g., which assessment methods and assessment objects are deemed to be the most useful in obtaining the desired results). This determination is made based on how the organization can accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the determination that the CUI requirements have been satisfied.

[6] Additional information on assessment methods and objects and the attributes of depth and coverage is provided in NIST Special Publication 800-53A.

2.2 ASSURANCE CASES

Building an effective assurance case for determining compliance to CUI security requirements is a process that involves compiling evidence from a variety of sources and conducting different types of activities during an assessment. An assurance case is a body of evidence organized into an argument demonstrating that some claim about a system is true. For assessments conducted using the procedures in this publication, that claim is *compliance* with the security requirements specified in NIST Special Publication 800-171. Assessors gather evidence during the assessment process to allow designated officials[7] to make objective determinations about compliance to the CUI security requirements. The evidence needed to make such determinations can be obtained from various sources including self-assessments, independent third-party assessments, or other types of assessments, depending on the needs of the organization establishing the requirements and the organization conducting the assessments.

For example, many technical security requirements are satisfied by security capabilities that are built in to commercial information technology products and systems. Product assessments are typically conducted by independent, third-party testing organizations.[8] These assessments examine the security functions of products and established configuration settings. Assessments can also be conducted to demonstrate compliance to industry, national, or international security standards as well as developer and vendor claims. Since many information technology products are assessed by commercial testing organizations and then subsequently deployed in hundreds of thousands of systems, these types of assessments can be carried out at a greater level of depth and provide deeper insights into the security capabilities of the products.

Ultimately, evidence needed to determine compliance comes from the implementation of the selected safeguards to satisfy the CUI security requirements and from the assessments of that implementation. Assessors can build on previously developed materials that started with the specification of the organization's information security needs and is further developed during the design, development, and implementation of the system and system components. These materials, developed while implementing security throughout the life cycle of the system, provide the initial evidence for an assurance case.

Assessments can be conducted by systems developers, systems integrators, auditors, system owners, or the security staffs of organizations. The assessors or assessment teams bring together available information about the system such as the results from individual component product assessments. The assessors can conduct additional system-level assessments using the procedures and methods contained in this publication and based on the implementation information provided by the nonfederal organization in its system security plan. System assessments can be used to compile and evaluate the evidence needed by organizations to help determine the effectiveness of the safeguards implemented to protect CUI; the actions needed to mitigate security-related risks to the organization; and compliance to the CUI security requirements.

[7] A *designated official* is an official, either internal or external to the nonfederal organization, with the responsibility to determine organizational compliance to CUI security requirements.

[8] Examples include Common Criteria Testing Laboratories evaluating commercial IT products in accordance with ISO/IEC 15408 and Cryptographic Module Validation Program Testing Laboratories evaluating cryptographic modules in accordance with Federal Information Processing Standard (FIPS) 140.

APPLICABLE CUI SECURITY REQUIREMENTS

The system security plan is used to describe how the organization meets or plans to meet the CUI security requirements. Any security requirements that are deemed *non-applicable* by the organization (e.g., no wireless capability in the system or the system component processing, storing, or transmitting CUI), are documented as such in the system security plan. Once the system security plan is completed, a security assessment plan can be developed using the assessment procedures described in Chapter Three and tailoring those procedures as needed. An assessment procedure is developed for every CUI security requirement that is applicable to the system, system component, or the organization. Conversely, security requirements that are deemed non-applicable in the system security plan are *not* assessed.

CHAPTER THREE

THE PROCEDURES

ASSESSMENT PROCEDURES, METHODS, AND OBJECTS FOR CUI SECURITY REQUIREMENTS

This chapter provides assessment procedures for all CUI security requirements defined in NIST Special Publication 800-171. The assessment procedures are organized into fourteen families. Organizations conducting CUI security requirement assessments can build their assessment plans using the information provided in the generic assessment procedures—selecting the specific assessment methods and objects that meet the organization's needs. Organizations also have flexibility in defining the level of rigor and detail associated with the assessment based on the assurance requirements of the organization. Appendix D provides additional information on the different levels of rigor and detail for assessments.

The assessment objective defined for each assessment procedure is achieved by applying the designated assessment methods to the selected assessment objects and compiling/producing the evidence necessary to make the determination associated with each assessment objective. Each determination statement contained within an assessment procedure produces one of the following findings: *satisfied* or *other than satisfied*. A finding of "satisfied" indicates that for the security requirement addressed by the determination statement, the assessment information obtained (i.e., the evidence collected) indicates that the assessment objective has been met producing a fully acceptable result. A finding of "other than satisfied" indicates that for the security requirement addressed by the determination statement, the assessment findings obtained indicate potential anomalies that may need to be addressed by the organization. A finding of "other than satisfied" may also indicate that for reasons specified in the assessment report, the assessor was unable to obtain sufficient information to make the determination called for in the determination statement.

For assessment findings that are other than satisfied, organizations may define subcategories of findings indicating the severity or criticality of the weaknesses or deficiencies discovered and the potential adverse effects of those weaknesses or deficiencies on organizational missions and/or business functions. Defining such subcategories can help to establish priorities for needed risk mitigation actions.

CAUTIONARY NOTE

The content in this publication can be used for many different assessment-related purposes in determining organizational compliance to the CUI security requirements. The broad range of potential assessment methods and objects listed in this publication do not necessarily reflect, and should not be directly associated with, actual compliance or noncompliance. Rather, the selection of specific assessment methods and objects from the list provided, can help generate a picture of overall compliance with the CUI security requirements. There is no expectation about the number of methods or objects needed to determine compliance to the CUI security requirements. Moreover, the entire list of potential assessment objects should not be viewed as required artifacts needed to determine compliance to the requirements. Organizations have the flexibility to determine the specific methods and objects sufficient to obtain the needed evidence to support claims of compliance.

3.1 ACCESS CONTROL

3.1.1	**SECURITY REQUIREMENT** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.1[a]	*authorized users are identified.*
	3.1.1[b]	*processes acting on behalf of authorized users are identified.*
	3.1.1[c]	*devices (and other systems) authorized to connect to the system are identified.*
	3.1.1[d]	*system access is limited to authorized users.*
	3.1.1[e]	*system access is limited to processes acting on behalf of authorized users.*
	3.1.1[f]	*system access is limited to authorized devices (including other systems).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management].	

3.1.2	**SECURITY REQUIREMENT** Limit system access to the types of transactions and functions that authorized users are permitted to execute.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.2[a]	*the types of transactions and functions that authorized users are permitted to execute are defined.*
	3.1.2[b]	*system access is limited to the defined types of transactions and functions for authorized users.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access enforcement; system security plan; system design documentation; list of approved authorizations including remote access authorizations; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with access enforcement responsibilities; system or network administrators; personnel with information security responsibilities; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing access control policy].	

3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

3.1.4	**SECURITY REQUIREMENT** Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.4[a]	*the duties of individuals requiring separation are defined.*
	3.1.4[b]	*responsibilities for duties that require separation are assigned to separate individuals.*
	3.1.4[c]	*access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing divisions of responsibility and separation of duties; system security plan; system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; system access authorizations; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for defining divisions of responsibility and separation of duties; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Mechanisms implementing separation of duties policy].	

3.1.5	**SECURITY REQUIREMENT** Employ the principle of least privilege, including for specific security functions and privileged accounts.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.5[a]	*privileged accounts are identified.*
	3.1.5[b]	*access to privileged accounts is authorized in accordance with the principle of least privilege.*
	3.1.5[c]	*security functions are identified.*
	3.1.5[d]	*access to security functions is authorized in accordance with the principle of least privilege.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; list of conditions for group and role membership; notifications or records of recently transferred, separated, or terminated employees; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring/audit records; procedures addressing least privilege; list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access is to be explicitly authorized; list of system-generated privileged accounts; list of system administration personnel; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities; personnel with responsibilities for defining least privileges necessary to accomplish specified tasks]. **Test**: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management; mechanisms implementing least privilege functions; mechanisms prohibiting privileged access to the system].	

3.1.6	**SECURITY REQUIREMENT** Use non-privileged accounts or roles when accessing nonsecurity functions.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.6[a]	*nonsecurity functions are identified.*
	3.1.6[b]	*users are required to use non-privileged accounts or roles when accessing nonsecurity functions.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing least privilege; system security plan; list of system-generated security functions assigned to system accounts or roles; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for defining least privileges necessary to accomplish specified organizational tasks; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Mechanisms implementing least privilege functions].	

3.1.7	**SECURITY REQUIREMENT** Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.7[a]	*privileged functions are defined.*
	3.1.7[b]	*non-privileged users are defined.*
	3.1.7[c]	*non-privileged users are prevented from executing privileged functions.*
	3.1.7[d]	*the execution of privileged functions is captured in audit logs.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing least privilege; system security plan; system design documentation; list of privileged functions and associated user account assignments; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; personnel with information security responsibilities; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing least privilege functions for non-privileged users; mechanisms auditing the execution of privileged functions].	

3.1.8	**SECURITY REQUIREMENT** Limit unsuccessful logon attempts.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.8[a]	*the means of limiting unsuccessful logon attempts is defined.*
	3.1.8[b]	*the defined means of limiting unsuccessful logon attempts is implemented.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing unsuccessful logon attempts; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with information security responsibilities; system developers; system or network administrators]. **Test**: [*SELECT FROM:* Mechanisms implementing access control policy for unsuccessful logon attempts].	

3.1.9	**SECURITY REQUIREMENT** Provide privacy and security notices consistent with applicable CUI rules.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.9[a]	*privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category.*

	3.1.9[b]	*privacy and security notices are displayed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Privacy and security policies, procedures addressing system use notification; documented approval of system use notification messages or banners; system audit logs and records; system design documentation; user acknowledgements of notification message or banner; system security plan; system use notification messages; system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel with responsibility for providing legal advice; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing system use notification].	

3.1.10	**SECURITY REQUIREMENT** Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.10[a]	*the period of inactivity after which the system initiates a session lock is defined.*
	3.1.10[b]	*access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity.*
	3.1.10[c]	*previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing session lock; procedures addressing identification and authentication; system design documentation; system configuration settings and associated documentation; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing access control policy for session lock].	

3.1.11	**SECURITY REQUIREMENT** Terminate (automatically) a user session after a defined condition.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.11[a]	*conditions requiring a user session to terminate are defined.*
	3.1.11[b]	*a user session is automatically terminated after any of the defined conditions occur.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing session termination; system design documentation; system security plan; system configuration settings and associated documentation; list of conditions or trigger events requiring session disconnect; system audit logs and records; other relevant documents or records].	

	Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing user session termination].

3.1.12	**SECURITY REQUIREMENT** Monitor and control remote access sessions.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.12[a]	*remote access sessions are permitted.*
	3.1.12[b]	*the types of permitted remote access are identified.*
	3.1.12[c]	*remote access sessions are controlled.*
	3.1.12[d]	*remote access sessions are monitored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access implementation and usage (including restrictions); configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; remote access authorizations; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for managing remote access connections; system or network administrators; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Remote access management capability for the system].	

3.1.13	**SECURITY REQUIREMENT** Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.13[a]	*cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.*
	3.1.13[b]	*cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the system; system security plan; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. **Test**: [*SELECT FROM:* Cryptographic mechanisms protecting remote access sessions].	

3.1.14	**SECURITY REQUIREMENT** Route remote access via managed access control points.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.14[a]	*managed access control points are identified and implemented.*
	3.1.14[b]	*remote access is routed through managed network access control points.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the system; system security plan; system design documentation; list of all managed network access control points; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Mechanisms routing all remote accesses through managed network access control points].	

3.1.15	**SECURITY REQUIREMENT** Authorize remote execution of privileged commands and remote access to security-relevant information.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.15[a]	*privileged commands authorized for remote execution are identified.*
	3.1.15[b]	*security-relevant information authorized to be accessed remotely is identified.*
	3.1.15[c]	*the execution of the identified privileged commands via remote access is authorized.*
	3.1.15[d]	*access to the identified security-relevant information via remote access is authorized.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the system; system configuration settings and associated documentation; system security plan; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Mechanisms implementing remote access management].	

3.1.16	**SECURITY REQUIREMENT** Authorize wireless access prior to allowing such connections.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.16[a]	*wireless access points are identified.*
	3.1.16[b]	*wireless access is authorized prior to allowing such connections.*

	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; configuration management plan; procedures addressing wireless access implementation and usage (including restrictions); system security plan; system design documentation; system configuration settings and associated documentation; wireless access authorizations; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for managing wireless access connections; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Wireless access management capability for the system].

3.1.17	**SECURITY REQUIREMENT** Protect wireless access using authentication and encryption.
	ASSESSMENT OBJECTIVE *Determine if:*
3.1.17[a]	*wireless access to the system is protected using authentication.*
3.1.17[b]	*wireless access to the system is protected using encryption.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; system design documentation; procedures addressing wireless implementation and usage (including restrictions); system security plan; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing wireless access protections to the system].

3.1.18	**SECURITY REQUIREMENT** Control connection of mobile devices.
	ASSESSMENT OBJECTIVE *Determine if:*
3.1.18[a]	*mobile devices that process, store, or transmit CUI are identified.*
3.1.18[b]	*mobile device connections are authorized.*
3.1.18[c]	*mobile device connections are monitored and logged.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; authorizations for mobile device connections to organizational systems; procedures addressing access control for mobile device usage (including restrictions); system design documentation; configuration management plan; system security plan; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel using mobile devices to access organizational systems; system or network administrators; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Access control capability authorizing mobile device connections to organizational systems].

3.1.19	**SECURITY REQUIREMENT** Encrypt CUI on mobile devices and mobile computing platforms.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.19[a]	*mobile devices and mobile computing platforms that process, store, or transmit CUI are identified.*
	3.1.19[b]	*encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access control for mobile devices; system design documentation; system configuration settings and associated documentation; encryption mechanisms and associated configuration documentation; system security plan; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with access control responsibilities for mobile devices; system or network administrators; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Encryption mechanisms protecting confidentiality of information on mobile devices].	

3.1.20	**SECURITY REQUIREMENT** Verify and control/limit connections to and use of external systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.20[a]	*connections to external systems are identified.*
	3.1.20[b]	*the use of external systems is identified.*
	3.1.20[c]	*connections to external systems are verified.*
	3.1.20[d]	*the use of external systems is verified.*
	3.1.20[e]	*connections to external systems are controlled/limited.*
	3.1.20[f]	*the use of external systems is controlled/limited.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the use of external systems; terms and conditions for external systems; system security plan; list of applications accessible from external systems; system configuration settings and associated documentation; system connection or processing agreements; account management documents; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for defining terms and conditions for use of external systems to access organizational systems; system or network administrators; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Mechanisms implementing terms and conditions on use of external systems].	

3.1.21	**SECURITY REQUIREMENT** Limit use of portable storage devices on external systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.21[a]	*the use of portable storage devices containing CUI on external systems is identified and documented.*
	3.1.21[b]	*limits on the use of portable storage devices containing CUI on external systems are defined.*
	3.1.21[c]	*the use of portable storage devices containing CUI on external systems is limited as defined.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the use of external systems; system security plan; system configuration settings and associated documentation; system connection or processing agreements; account management documents; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for restricting or prohibiting use of organization-controlled storage devices on external systems; system or network administrators; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Mechanisms implementing restrictions on use of portable storage devices].	

3.1.22	**SECURITY REQUIREMENT** Control CUI posted or processed on publicly accessible systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.22[a]	*individuals authorized to post or process information on publicly accessible systems are identified.*
	3.1.22[b]	*procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.*
	3.1.22[c]	*a review process is in place prior to posting of any content to publicly accessible systems.*
	3.1.22[d]	*content on publicly accessible systems is reviewed to ensure that it does not include CUI.*
	3.1.22[e]	*mechanisms are in place to remove and address improper posting of CUI.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing publicly accessible content; system security plan; list of users authorized to post publicly accessible content on organizational systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs and records; security awareness training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for managing publicly accessible information posted on organizational systems; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Mechanisms implementing management of publicly accessible content].	

3.2 AWARENESS AND TRAINING

3.2.1	**SECURITY REQUIREMENT** Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.2.1[a]	*security risks associated with organizational activities involving CUI are identified.*
	3.2.1[b]	*policies, standards, and procedures related to the security of the system are identified.*
	3.2.1[c]	*managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.*
	3.2.1[d]	*managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; relevant codes of federal regulations; security awareness training curriculum; security awareness training materials; system security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for security awareness training; personnel with information security responsibilities; personnel composing the general system user community; personnel with responsibilities for role-based awareness training]. **Test**: [*SELECT FROM:* Mechanisms managing security awareness training; mechanisms managing role-based security training].	

3.2.2	**SECURITY REQUIREMENT** Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.2.2[a]	*information security-related duties, roles, and responsibilities are defined.*
	3.2.2[b]	*information security-related duties, roles, and responsibilities are assigned to designated personnel.*
	3.2.2[c]	*personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; system security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for role-based security training; personnel with assigned system security roles and responsibilities; personnel with responsibilities	

	for security awareness training; personnel with information security responsibilities; personnel representing the general system user community]. **Test**: [*SELECT FROM:* Mechanisms managing role-based security training; mechanisms managing security awareness training].

3.2.3	**SECURITY REQUIREMENT** Provide security awareness training on recognizing and reporting potential indicators of insider threat.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.2.3[a]	*potential indicators associated with insider threats are identified.*
	3.2.3[b]	*security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; insider threat policy and procedures; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel that participate in security awareness training; personnel with responsibilities for basic security awareness training; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Mechanisms managing insider threat training].	

3.3 AUDIT AND ACCOUNTABILITY

3.3.1	**SECURITY REQUIREMENT** Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.3.1[a]	*audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.*
	3.3.1[b]	*the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.*
	3.3.1[c]	*audit records are created (generated).*
	3.3.1[d]	*audit records, once created, contain the defined content.*
	3.3.1[e]	*retention requirements for audit records are defined.*
	3.3.1[f]	*audit records are retained as defined.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing auditable events; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing control of audit records; procedures addressing audit record generation; system audit logs and records; system auditable events; system incident reports; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; personnel with audit review, analysis and reporting responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Mechanisms implementing system audit logging].	

3.3.2	**SECURITY REQUIREMENT** Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.3.2[a]	*the content of the audit records needed to support the ability to uniquely trace users to their actions is defined.*
	3.3.2[b]	*audit records, once created, contain the defined content.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit records and event types; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing audit record generation; procedures addressing audit review, analysis, and reporting; reports of audit findings; system audit logs and records; system events; system incident reports; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators].	

	Test: [*SELECT FROM:* Mechanisms implementing system audit logging].

3.3.3	**SECURITY REQUIREMENT** Review and update logged events.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.3.3[a]	*a process for determining when to review logged events is defined.*
	3.3.3[b]	*event types being logged are reviewed in accordance with the defined review process.*
	3.3.3[c]	*event types being logged are updated based on the review.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit records and event types; system security plan; list of organization-defined event types to be logged; reviewed and updated records of logged event types; system audit logs and records; system incident reports; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Mechanisms supporting review and update of logged event types].	

3.3.4	**SECURITY REQUIREMENT** Alert in the event of an audit logging process failure.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.3.4[a]	*personnel or roles to be alerted in the event of an audit logging process failure are identified.*
	3.3.4[b]	*types of audit logging process failures for which alert will be generated are defined.*
	3.3.4[c]	*identified personnel or roles are alerted in the event of an audit logging process failure.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing response to audit logging processing failures; system design documentation; system security plan; system configuration settings and associated documentation; list of personnel to be notified in case of an audit logging processing failure; system incident reports; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing system response to audit logging processing failures].	

3.3.5	**SECURITY REQUIREMENT** Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.3.5[a]	*audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined.*
	3.3.5[b]	*defined audit record review, analysis, and reporting processes are correlated.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit record review, analysis, and reporting; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing investigation of and response to suspicious activities; system audit logs and records across different repositories; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with audit record review, analysis, and reporting responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Mechanisms supporting analysis and correlation of audit records; mechanisms integrating audit review, analysis and reporting].	

3.3.6	**SECURITY REQUIREMENT** Provide audit record reduction and report generation to support on-demand analysis and reporting.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.3.6[a]	*an audit record reduction capability that supports on-demand analysis is provided.*
	3.3.6[b]	*a report generation capability that supports on-demand reporting is provided.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit record reduction and report generation; system design documentation; system security plan; system configuration settings and associated documentation; audit record reduction, review, analysis, and reporting tools; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with audit record reduction and report generation responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Audit record reduction and report generation capability].	

3.3.7	**SECURITY REQUIREMENT** Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.3.7[a]	*internal system clocks are used to generate time stamps for audit records.*

	3.3.7[b]	*an authoritative source with which to compare and synchronize internal system clocks is specified.*
	3.3.7[c]	*internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing time stamp generation; system design documentation; system security plan; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing time stamp generation; mechanisms implementing internal information system clock synchronization].	

3.3.8	**SECURITY REQUIREMENT** Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
	ASSESSMENT OBJECTIVE *Determine if:*
3.3.8[a]	*audit information is protected from unauthorized access.*
3.3.8[b]	*audit information is protected from unauthorized modification.*
3.3.8[c]	*audit information is protected from unauthorized deletion.*
3.3.8[d]	*audit logging tools are protected from unauthorized access.*
3.3.8[e]	*audit logging tools are protected from unauthorized modification.*
3.3.8[f]	*audit logging tools are protected from unauthorized deletion.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Audit and accountability policy; access control policy and procedures; procedures addressing protection of audit information; system security plan; system design documentation; system configuration settings and associated documentation, system audit logs and records; audit logging tools; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing audit information protection].

3.3.9	**SECURITY REQUIREMENT** Limit management of audit logging functionality to a subset of privileged users.
	ASSESSMENT OBJECTIVE *Determine if:*
3.3.9[a]	*a subset of privileged users granted access to manage audit logging functionality is defined.*
3.3.9[b]	*management of audit logging functionality is limited to the defined subset of privileged users.*

	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Audit and accountability policy; access control policy and procedures; procedures addressing protection of audit information; system security plan; system design documentation; system configuration settings and associated documentation; access authorizations; system-generated list of privileged users with access to management of audit logging functionality; access control list; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms managing access to audit logging functionality].

3.4 CONFIGURATION MANAGEMENT

3.4.1	**SECURITY REQUIREMENT** Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.4.1[a]	*a baseline configuration is established.*
	3.4.1[b]	*the baseline configuration includes hardware, software, firmware, and documentation.*
	3.4.1[c]	*the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.*
	3.4.1[d]	*a system inventory is established.*
	3.4.1[e]	*the system inventory includes hardware, software, firmware, and documentation.*
	3.4.1[f]	*the inventory is maintained (reviewed and updated) throughout the system development life cycle.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing the baseline configuration of the system; procedures addressing system inventory; system security plan; configuration management plan; system inventory records; inventory review and update records; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system component installation records; system component removal records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with configuration management responsibilities; personnel with responsibilities for establishing the system inventory; personnel with responsibilities for updating the system inventory; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for managing baseline configurations; mechanisms supporting configuration control of the baseline configuration; organizational processes for developing and documenting an inventory of system components; organizational processes for updating inventory of system components; mechanisms supporting or implementing the system inventory; mechanisms implementing updating of the system inventory].	

3.4.2	**SECURITY REQUIREMENT** Establish and enforce security configuration settings for information technology products employed in organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.4.2[a]	*security configuration settings for information technology products employed in the system are established and included in the baseline configuration.*
	3.4.2[b]	*security configuration settings for information technology products employed in the system are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS	

	Examine: [*SELECT FROM:* Configuration management policy; baseline configuration; procedures addressing configuration settings for the system; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; security configuration checklists; evidence supporting approved deviations from established configuration settings; change control records; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with security configuration management responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for managing configuration settings; mechanisms that implement, monitor, and/or control system configuration settings; mechanisms that identify and/or document deviations from established configuration settings; processes for managing baseline configurations; mechanisms supporting configuration control of baseline configurations].

3.4.3	**SECURITY REQUIREMENT** Track, review, approve or disapprove, and log changes to organizational systems.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.4.3[a] *changes to the system are tracked.*
	3.4.3[b] *changes to the system are reviewed.*
	3.4.3[c] *changes to the system are approved or disapproved.*
	3.4.3[d] *changes to the system are logged.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing system configuration change control; configuration management plan; system architecture and configuration documentation; system security plan; change control records; system audit logs and records; change control audit and review reports; agenda/minutes from configuration change control oversight meetings; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with configuration change control responsibilities; personnel with information security responsibilities; system or network administrators; members of change control board or similar]. **Test**: [*SELECT FROM:* Organizational processes for configuration change control; mechanisms that implement configuration change control].

3.4.4	**SECURITY REQUIREMENT** Analyze the security impact of changes prior to implementation.
	ASSESSMENT OBJECTIVE *Determine if the security impact of changes to the system is analyzed prior to implementation.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing security impact analysis for system changes; configuration management plan; security impact analysis documentation; system security plan; analysis tools and associated outputs; change control records; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibility for conducting security impact analysis; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for security impact analysis].

3.4.5	**SECURITY REQUIREMENT** Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.4.5[a]	*physical access restrictions associated with changes to the system are defined.*
	3.4.5[b]	*physical access restrictions associated with changes to the system are documented.*
	3.4.5[c]	*physical access restrictions associated with changes to the system are approved.*
	3.4.5[d]	*physical access restrictions associated with changes to the system are enforced.*
	3.4.5[e]	*logical access restrictions associated with changes to the system are defined.*
	3.4.5[f]	*logical access restrictions associated with changes to the system are documented.*
	3.4.5[g]	*logical access restrictions associated with changes to the system are approved.*
	3.4.5[h]	*logical access restrictions associated with changes to the system are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing access restrictions for changes to the system; system security plan; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; logical access approvals; physical access approvals; access credentials; change control records; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with logical access control responsibilities; personnel with physical access control responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for managing access restrictions associated with changes to the system; mechanisms supporting, implementing, and enforcing access restrictions associated with changes to the system].	

3.4.6	**SECURITY REQUIREMENT** Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.4.6[a]	*essential system capabilities are defined based on the principle of least functionality.*
	3.4.6[b]	*the system is configured to provide only the defined essential capabilities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing least functionality in the system; system security plan; system design documentation; system configuration settings and associated documentation; security configuration checklists; other relevant documents or records].	

	Interview: [*SELECT FROM:* Personnel with security configuration management responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes prohibiting or restricting functions, ports, protocols, or services; mechanisms implementing restrictions or prohibition of functions, ports, protocols, or services].

3.4.7	**SECURITY REQUIREMENT** Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.4.7[a] *essential programs are defined.*
	3.4.7[b] *the use of nonessential programs is defined.*
	3.4.7[c] *the use of nonessential programs is restricted, disabled, or prevented as defined.*
	3.4.7[d] *essential functions are defined.*
	3.4.7[e] *the use of nonessential functions is defined.*
	3.4.7[f] *the use of nonessential functions is restricted, disabled, or prevented as defined.*
	3.4.7[g] *essential ports are defined.*
	3.4.7[h] *the use of nonessential ports is defined.*
	3.4.7[i] *the use of nonessential ports is restricted, disabled, or prevented as defined.*
	3.4.7[j] *essential protocols are defined.*
	3.4.7[k] *the use of nonessential protocols is defined.*
	3.4.7[l] *the use of nonessential protocols is restricted, disabled, or prevented as defined.*
	3.4.7[m] *essential services are defined.*
	3.4.7[n] *the use of nonessential services is defined.*
	3.4.7[o] *the use of nonessential services is restricted, disabled, or prevented as defined.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system security plan; system design documentation; security configuration checklists; system configuration settings and associated documentation; specifications for preventing software program execution; documented reviews of programs, functions, ports, protocols, and/or services; change control records; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for reviewing programs, functions, ports, protocols, and services on the system; personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Organizational processes for reviewing and disabling nonessential programs, functions, ports, protocols, or services; mechanisms implementing review and handling of nonessential programs, functions, ports, protocols, or services; organizational processes preventing program execution on the system; organizational processes for software program usage and restrictions; mechanisms supporting or implementing software program usage and restrictions; mechanisms preventing program execution on the system].

3.4.8	**SECURITY REQUIREMENT** Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.4.8[a] *a policy specifying whether whitelisting or blacklisting is to be implemented is specified.*
	3.4.8[b] *the software allowed to execute under whitelisting or denied use under blacklisting is specified.*
	3.4.8[c] *whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing least functionality in the system; system security plan; configuration management plan; system design documentation; system configuration settings and associated documentation; list of software programs not authorized to execute on the system; list of software programs authorized to execute on the system; security configuration checklists; review and update records associated with list of authorized or unauthorized software programs; change control records; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for identifying software authorized or not authorized to execute on the system; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational process for identifying, reviewing, and updating programs authorized or not authorized to execute on the system; process for implementing blacklisting or whitelisting; mechanisms supporting or implementing blacklisting or whitelisting].

3.4.9	**SECURITY REQUIREMENT** Control and monitor user-installed software.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.4.9[a] *a policy for controlling the installation of software by users is established.*
	3.4.9[b] *installation of software by users is controlled based on the established policy.*
	3.4.9[c] *installation of software by users is monitored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing user installed software; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; list of rules governing user-installed software; system monitoring records; system audit logs and records; continuous monitoring strategy; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for governing user-installed software; personnel operating, using, or maintaining the system; personnel monitoring compliance with user-installed software policy; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes governing user-installed software on the system; mechanisms enforcing rules or methods for governing the installation of software by users; mechanisms monitoring policy compliance].

3.5 IDENTIFICATION AND AUTHENTICATION

3.5.1	**SECURITY REQUIREMENT** Identify system users, processes acting on behalf of users, and devices.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.5.1[a]	*system users are identified.*
	3.5.1[b]	*processes acting on behalf of users are identified.*
	3.5.1[c]	*devices accessing the system are identified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; system security plan, system design documentation; system configuration settings and associated documentation; system audit logs and records; list of system accounts; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system operations responsibilities; personnel with information security responsibilities; system or network administrators; personnel with account management responsibilities; system developers]. **Test**: [*SELECT FROM:* Organizational processes for uniquely identifying and authenticating users; mechanisms supporting or implementing identification and authentication capability].	

3.5.2	**SECURITY REQUIREMENT** Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.5.2[a]	*the identity of each user is authenticated or verified as a prerequisite to system access.*
	3.5.2[b]	*the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.*
	3.5.2[c]	*the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; system security plan; procedures addressing authenticator management; procedures addressing user identification and authentication; system design documentation; list of system authenticator types; system configuration settings and associated documentation; change control records associated with managing system authenticators; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Mechanisms supporting or implementing authenticator management capability].	

3.5.3	**SECURITY REQUIREMENT** Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.5.3[a]	*privileged accounts are identified.*
	3.5.3[b]	*multifactor authentication is implemented for local access to privileged accounts.*
	3.5.3[c]	*multifactor authentication is implemented for network access to privileged accounts.*
	3.5.3[d]	*multifactor authentication is implemented for network access to non-privileged accounts.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; list of system accounts; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system operations responsibilities; personnel with account management responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms supporting or implementing multifactor authentication capability].	

3.5.4	**SECURITY REQUIREMENT** Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	
	ASSESSMENT OBJECTIVE *Determine if replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts.*	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; list of privileged system accounts; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system operations responsibilities; personnel with account management responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms supporting or implementing identification and authentication capability or replay resistant authentication mechanisms].	

3.5.5	**SECURITY REQUIREMENT** Prevent reuse of identifiers for a defined period.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.5.5[a]	*a period within which identifiers cannot be reused is defined.*

	3.5.5[b]	*reuse of identifiers is prevented within the defined period.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of system accounts; list of identifiers generated from physical access control devices; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with identifier management responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms supporting or implementing identifier management].	

3.5.6	**SECURITY REQUIREMENT** Disable identifiers after a defined period of inactivity.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.5.6[a]	*a period of inactivity after which an identifier is disabled is defined.*
	3.5.6[b]	*identifiers are disabled after the defined period of inactivity.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of system accounts; list of identifiers generated from physical access control devices; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with identifier management responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms supporting or implementing identifier management].	

3.5.7	**SECURITY REQUIREMENT** Enforce a minimum password complexity and change of characters when new passwords are created.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.5.7[a]	*password complexity requirements are defined.*
	3.5.7[b]	*password change of character requirements are defined.*
	3.5.7[c]	*minimum password complexity requirements as defined are enforced when new passwords are created.*
	3.5.7[d]	*minimum password change of character requirements as defined are enforced when new passwords are created.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system configuration settings and associated documentation; system design documentation; password configurations and associated documentation; other relevant documents or records].	

	Interview: [*SELECT FROM:* Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms supporting or implementing password-based authenticator management capability].

3.5.8	**SECURITY REQUIREMENT** Prohibit password reuse for a specified number of generations.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.5.8[a] *the number of generations during which a password cannot be reused is specified.*
	3.5.8[b] *reuse of passwords is prohibited during the specified number of generations.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system design documentation; system configuration settings and associated documentation; password configurations and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms supporting or implementing password-based authenticator management capability].

3.5.9	**SECURITY REQUIREMENT** Allow temporary password use for system logons with an immediate change to a permanent password.
	ASSESSMENT OBJECTIVE *Determine if an immediate change to a permanent password is required when a temporary password is used for system logon.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system configuration settings and associated documentation; system design documentation; password configurations and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms supporting or implementing password-based authenticator management capability].

3.5.10	**SECURITY REQUIREMENT** Store and transmit only cryptographically-protected passwords.
	ASSESSMENT OBJECTIVE *Determine if:*

	3.5.10[a]	*passwords are cryptographically protected in storage.*
	3.5.10[b]	*passwords are cryptographically protected in transit.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system configuration settings and associated documentation; system design documentation; password configurations and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms supporting or implementing password-based authenticator management capability].	

3.5.11	**SECURITY REQUIREMENT** Obscure feedback of authentication information.
	ASSESSMENT OBJECTIVE *Determine if authentication information is obscured during the authentication process.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator feedback; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with information security responsibilities; system or network administrators; system developers]. **Test**: [*SELECT FROM:* Mechanisms supporting or implementing the obscuring of feedback of authentication information during authentication].

3.6 INCIDENT RESPONSE

3.6.1	**SECURITY REQUIREMENT** Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.6.1[a]	*an operational incident-handling capability is established.*
	3.6.1[b]	*the operational incident-handling capability includes preparation.*
	3.6.1[c]	*the operational incident-handling capability includes detection.*
	3.6.1[d]	*the operational incident-handling capability includes analysis.*
	3.6.1[e]	*the operational incident-handling capability includes containment.*
	3.6.1[f]	*the operational incident-handling capability includes recovery.*
	3.6.1[g]	*the operational incident-handling capability includes user response activities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Incident response policy; contingency planning policy; procedures addressing incident handling; procedures addressing incident response assistance; incident response plan; contingency plan; system security plan; procedures addressing incident response training; incident response training curriculum; incident response training materials; incident response training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with incident handling responsibilities; personnel with contingency planning responsibilities; personnel with incident response training and operational responsibilities; personnel with incident response assistance and support responsibilities; personnel with access to incident response support and assistance capability; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Incident-handling capability for the organization; organizational processes for incident response assistance; mechanisms supporting or implementing incident response assistance].	

3.6.2	**SECURITY REQUIREMENT** Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.6.2[a]	*incidents are tracked.*
	3.6.2[b]	*incidents are documented.*
	3.6.2[c]	*authorities to whom incidents are to be reported are identified.*
	3.6.2[d]	*organizational officials to whom incidents are to be reported are identified.*
	3.6.2[e]	*identified authorities are notified of incidents.*
	3.6.2[f]	*identified organizational officials are notified of incidents.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS	

	Examine: [*SELECT FROM:* Incident response policy; procedures addressing incident monitoring; incident response records and documentation; procedures addressing incident reporting; incident reporting records and documentation; incident response plan; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with incident monitoring responsibilities; personnel with incident reporting responsibilities; personnel who have or should have reported incidents; personnel (authorities) to whom incident information is to be reported; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Incident monitoring capability for the organization; mechanisms supporting or implementing tracking and documenting of system security incidents; organizational processes for incident reporting; mechanisms supporting or implementing incident reporting].

3.6.3	**SECURITY REQUIREMENT** Test the organizational incident response capability.
	ASSESSMENT OBJECTIVE *Determine if the incident response capability is tested.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Incident response policy; contingency planning policy; procedures addressing incident response testing; procedures addressing contingency plan testing; incident response testing material; incident response test results; incident response test plan; incident response plan; contingency plan; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with incident response testing responsibilities; personnel with information security responsibilities; personnel with responsibilities for testing plans related to incident response]. **Test**: [*SELECT FROM:* Mechanisms and processes for incident response].

3.7 MAINTENANCE

3.7.1	**SECURITY REQUIREMENT** Perform maintenance on organizational systems.
	ASSESSMENT OBJECTIVE *Determine if system maintenance is performed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for systems; organizational processes for sanitizing system components; mechanisms supporting or implementing controlled maintenance; mechanisms implementing sanitization of system components].

3.7.2	**SECURITY REQUIREMENT** Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.7.2[a]	*tools used to conduct system maintenance are controlled.*
	3.7.2[b]	*techniques used to conduct system maintenance are controlled.*
	3.7.2[c]	*mechanisms used to conduct system maintenance are controlled.*
	3.7.2[d]	*personnel used to conduct system maintenance are controlled.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System maintenance policy; procedures addressing system maintenance tools and media; maintenance records; system maintenance tools and associated documentation; maintenance tool inspection records; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for approving, controlling, and monitoring maintenance tools; mechanisms supporting or implementing approval, control, and monitoring of maintenance tools; organizational processes for inspecting maintenance tools; mechanisms supporting or implementing inspection of maintenance tools; organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance].	

3.7.3	**SECURITY REQUIREMENT** Ensure equipment removed for off-site maintenance is sanitized of any CUI.
	ASSESSMENT OBJECTIVE *Determine if equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for systems; organizational processes for sanitizing system components; mechanisms supporting or implementing controlled maintenance; mechanisms implementing sanitization of system components].

3.7.4	**SECURITY REQUIREMENT** Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
	ASSESSMENT OBJECTIVE *Determine if media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance].

3.7.5	**SECURITY REQUIREMENT** Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.7.5[a]	*multifactor authentication is used to establish nonlocal maintenance sessions via external network connections.*
	3.7.5[b]	*nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System maintenance policy; procedures addressing nonlocal system maintenance; system security plan; system design documentation; system configuration	

	settings and associated documentation; maintenance records; diagnostic records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for managing nonlocal maintenance; mechanisms implementing, supporting, and managing nonlocal maintenance; mechanisms for strong authentication of nonlocal maintenance diagnostic sessions; mechanisms for terminating nonlocal maintenance sessions and network connections].

3.7.6	**SECURITY REQUIREMENT** Supervise the maintenance activities of maintenance personnel without required access authorization.
	ASSESSMENT OBJECTIVE *Determine if maintenance personnel without required access authorization are supervised during maintenance activities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System maintenance policy; procedures addressing maintenance personnel; service provider contracts; service-level agreements; list of authorized personnel; maintenance records; access control records; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for authorizing and managing maintenance personnel; mechanisms supporting or implementing authorization of maintenance personnel].

3.8 MEDIA PROTECTION

3.8.1	**SECURITY REQUIREMENT** Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.8.1[a]	*paper media containing CUI is physically controlled.*
	3.8.1[b]	*digital media containing CUI is physically controlled.*
	3.8.1[c]	*paper media containing CUI is securely stored.*
	3.8.1[d]	*digital media containing CUI is securely stored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; procedures addressing media storage; procedures addressing media access restrictions; access control policy and procedures; physical and environmental protection policy and procedures; system security plan; media storage facilities; access control records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system media protection responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for restricting information media; mechanisms supporting or implementing media access restrictions].	

3.8.2	**SECURITY REQUIREMENT** Limit access to CUI on system media to authorized users.
	ASSESSMENT OBJECTIVE *Determine if access to CUI on system media is limited to authorized users.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; system media; designated controlled areas; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system media protection and storage responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for storing media; mechanisms supporting or implementing secure media storage and media protection].

3.8.3	**SECURITY REQUIREMENT** Sanitize or destroy system media containing CUI before disposal or release for reuse.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.8.3[a]	*system media containing CUI is sanitized or destroyed before disposal.*
	3.8.3[b]	*system media containing CUI is sanitized before it is released for reuse.*

	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; procedures addressing media sanitization and disposal; applicable standards and policies addressing media sanitization; system security plan; media sanitization records; system audit logs and records; system design documentation; system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with media sanitization responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for media sanitization; mechanisms supporting or implementing media sanitization].

3.8.4	**SECURITY REQUIREMENT** Mark media with necessary CUI markings and distribution limitations.
	ASSESSMENT OBJECTIVE *Determine if:*
3.8.4[a]	*media containing CUI is marked with applicable CUI markings.*
3.8.4[b]	*media containing CUI is marked with distribution limitations.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; procedures addressing media marking; physical and environmental protection policy and procedures; system security plan; list of system media marking security attributes; designated controlled areas; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system media protection and marking responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for marking information media; mechanisms supporting or implementing media marking].

3.8.5	**SECURITY REQUIREMENT** Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
	ASSESSMENT OBJECTIVE *Determine if:*
3.8.5[a]	*access to media containing CUI is controlled.*
3.8.5[b]	*accountability for media containing CUI is maintained during transport outside of controlled areas.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; system media; designated controlled areas; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system media protection and storage responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for storing media; mechanisms supporting or implementing media storage and media protection].

3.8.6	**SECURITY REQUIREMENT** Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
	ASSESSMENT OBJECTIVE *Determine if the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; procedures addressing media transport; system design documentation; system security plan; system configuration settings and associated documentation; system media transport records; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system media transport responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Cryptographic mechanisms protecting information on digital media during transportation outside controlled areas].

3.8.7	**SECURITY REQUIREMENT** Control the use of removable media on system components.
	ASSESSMENT OBJECTIVE *Determine if the use of removable media on system components is controlled.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; system use policy; procedures addressing media usage restrictions; system security plan; rules of behavior; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system media use responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for media use; mechanisms restricting or prohibiting use of system media on systems or system components].

3.8.8	**SECURITY REQUIREMENT** Prohibit the use of portable storage devices when such devices have no identifiable owner.
	ASSESSMENT OBJECTIVE *Determine if the use of portable storage devices is prohibited when such devices have no identifiable owner.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; system use policy; procedures addressing media usage restrictions; system security plan; rules of behavior; system configuration settings and associated documentation; system design documentation; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system media use responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for media use; mechanisms prohibiting use of media on systems or system components].

3.8.9	**SECURITY REQUIREMENT** Protect the confidentiality of backup CUI at storage locations.
	ASSESSMENT OBJECTIVE *Determine if the confidentiality of backup CUI is protected at storage locations.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Procedures addressing system backup; system configuration settings and associated documentation; security plan; backup storage locations; system backup logs or records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system backup responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for conducting system backups; mechanisms supporting or implementing system backups].

3.9 PERSONNEL SECURITY

3.9.1	**SECURITY REQUIREMENT** Screen individuals prior to authorizing access to organizational systems containing CUI.
	ASSESSMENT OBJECTIVE *Determine if individuals are screened prior to authorizing access to organizational systems containing CUI.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing personnel screening; records of screened personnel; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with personnel security responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for personnel screening].

3.9.2	**SECURITY REQUIREMENT** Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.9.2[a]	*a policy and/or process for terminating system access and any credentials coincident with personnel actions is established.*
	3.9.2[b]	*system access and credentials are terminated consistent with personnel actions such as termination or transfer.*
	3.9.2[c]	*the system is protected during and after personnel transfer actions.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing personnel transfer and termination; records of personnel transfer and termination actions; list of system accounts; records of terminated or revoked authenticators and credentials; records of exit interviews; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with personnel security responsibilities; personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for personnel transfer and termination; mechanisms supporting or implementing personnel transfer and termination notifications; mechanisms for disabling system access and revoking authenticators].	

3.10 PHYSICAL PROTECTION

3.10.1	**SECURITY REQUIREMENT** Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.10.1[a] *authorized individuals allowed physical access are identified.*
	3.10.1[b] *physical access to organizational systems is limited to authorized individuals.*
	3.10.1[c] *physical access to equipment is limited to authorized individuals.*
	3.10.1[d] *physical access to operating environments is limited to authorized individuals.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; system security plan; authorized personnel access list; authorization credentials; physical access list reviews; physical access termination records and associated documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with physical access authorization responsibilities; personnel with physical access to system facility; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for physical access authorizations; mechanisms supporting or implementing physical access authorizations].

3.10.2	**SECURITY REQUIREMENT** Protect and monitor the physical facility and support infrastructure for organizational systems.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.10.2[a] *the physical facility where organizational systems reside is protected.*
	3.10.2[b] *the support infrastructure for organizational systems is protected.*
	3.10.2[c] *the physical facility where organizational systems reside is monitored.*
	3.10.2[d] *the support infrastructure for organizational systems is monitored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access monitoring; system security plan; physical access logs or records; physical access monitoring records; physical access log reviews; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with physical access monitoring responsibilities; personnel with incident response responsibilities; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for monitoring physical access; mechanisms supporting or implementing physical access monitoring; mechanisms supporting or implementing the review of physical access logs].

3.10.3	**SECURITY REQUIREMENT** Escort visitors and monitor visitor activity.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.10.3[a]	*visitors are escorted.*
	3.10.3[b]	*visitor activity is monitored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with physical access control responsibilities; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices].	

3.10.4	**SECURITY REQUIREMENT** Maintain audit logs of physical access.
	ASSESSMENT OBJECTIVE *Determine if audit logs of physical access are maintained.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with physical access control responsibilities; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices].

3.10.5	**SECURITY REQUIREMENT** Control and manage physical access devices.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.10.5[a]	*physical access devices are identified.*
	3.10.5[b]	*physical access devices are controlled.*
	3.10.5[c]	*physical access devices are managed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records;	

	inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with physical access control responsibilities; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices].

3.10.6	**SECURITY REQUIREMENT** Enforce safeguarding measures for CUI at alternate work sites.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.10.6[a] *safeguarding measures for CUI are defined for alternate work sites.*
	3.10.6[b] *safeguarding measures for CUI are enforced for alternate work sites.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing alternate work sites for personnel; system security plan; list of safeguards required for alternate work sites; assessments of safeguards at alternate work sites; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel approving use of alternate work sites; personnel using alternate work sites; personnel assessing controls at alternate work sites; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for security at alternate work sites; mechanisms supporting alternate work sites; safeguards employed at alternate work sites; means of communications between personnel at alternate work sites and security personnel].

3.11 RISK ASSESSMENT

3.11.1	**SECURITY REQUIREMENT** Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.11.1[a]	*the frequency to assess risk to organizational operations, organizational assets, and individuals is defined.*
	3.11.1[b]	*risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Risk assessment policy; security planning policy and procedures; procedures addressing organizational risk assessments; system security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with risk assessment responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for risk assessment; mechanisms supporting or for conducting, documenting, reviewing, disseminating, and updating the risk assessment].	

3.11.2	**SECURITY REQUIREMENT** Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.11.2[a]	*the frequency to scan for vulnerabilities in organizational systems and applications is defined.*
	3.11.2[b]	*vulnerability scans are performed on organizational systems with the defined frequency.*
	3.11.2[c]	*vulnerability scans are performed on applications with the defined frequency.*
	3.11.2[d]	*vulnerability scans are performed on organizational systems when new vulnerabilities are identified.*
	3.11.2[e]	*vulnerability scans are performed on applications when new vulnerabilities are identified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis and remediation responsibilities; personnel with information security responsibilities; system or network administrators].	

	Test: [*SELECT FROM:* Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting or implementing vulnerability scanning, analysis, remediation, and information sharing].

3.11.3	**SECURITY REQUIREMENT** Remediate vulnerabilities in accordance with risk assessments.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.11.3[a]	*vulnerabilities are identified.*
	3.11.3[b]	*vulnerabilities are remediated in accordance with risk assessments.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis responsibilities; personnel with vulnerability remediation responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting or implementing vulnerability scanning, analysis, remediation, and information sharing].	

3.12 SECURITY ASSESSMENT

3.12.1	**SECURITY REQUIREMENT** Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.12.1[a]	*the frequency of security control assessments is defined.*
	3.12.1[b]	*security controls are assessed with the defined frequency to determine if the controls are effective in their application.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security assessment planning; procedures addressing security assessments; security assessment plan; system security plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with security assessment responsibilities; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Mechanisms supporting security assessment, security assessment plan development, and security assessment reporting].	

3.12.2	**SECURITY REQUIREMENT** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.12.2[a]	*deficiencies and vulnerabilities to be addressed by the plan of action are identified.*
	3.12.2[b]	*a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.*
	3.12.2[c]	*the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Security assessment and authorization policy; procedures addressing plan of action; system security plan; security assessment plan; security assessment report; security assessment evidence; plan of action; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with plan of action development and implementation responsibilities; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Mechanisms for developing, implementing, and maintaining plan of action].	

3.12.3	**SECURITY REQUIREMENT** Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
	ASSESSMENT OBJECTIVE *Determine if security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Security planning policy; organizational procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan].

3.12.4	**SECURITY REQUIREMENT** Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.12.4[a]	*a system security plan is developed.*
	3.12.4[b]	*the system boundary is described and documented in the system security plan.*
	3.12.4[c]	*the system environment of operation is described and documented in the system security plan.*
	3.12.4[d]	*the security requirements identified and approved by the designated authority as non-applicable are identified.*
	3.12.4[e]	*the method of security requirement implementation is described and documented in the system security plan.*
	3.12.4[f]	*the relationship with or connection to other systems is described and documented in the system security plan.*
	3.12.4[g]	*the frequency to update the system security plan is defined.*
	3.12.4[h]	*system security plan is updated with the defined frequency.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Security planning policy; procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan].	

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

3.13.1	**SECURITY REQUIREMENT** Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.13.1[a]	*the external system boundary is defined.*
	3.13.1[b]	*key internal system boundaries are defined.*
	3.13.1[c]	*communications are monitored at the external system boundary.*
	3.13.1[d]	*communications are monitored at key internal boundaries.*
	3.13.1[e]	*communications are controlled at the external system boundary.*
	3.13.1[f]	*communications are controlled at key internal boundaries.*
	3.13.1[g]	*communications are protected at the external system boundary.*
	3.13.1[h]	*communications are protected at key internal boundaries.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; system security plan; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; enterprise security architecture documentation; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer; personnel with boundary protection responsibilities]. **Test:** [*SELECT FROM:* Mechanisms implementing boundary protection capability].	

3.13.2	**SECURITY REQUIREMENT** Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.13.2[a]	*architectural designs that promote effective information security are identified.*
	3.13.2[b]	*software development techniques that promote effective information security are identified.*
	3.13.2[c]	*systems engineering principles that promote effective information security are identified.*
	3.13.2[d]	*identified architectural designs that promote effective information security are employed.*
	3.13.2[e]	*identified software development techniques that promote effective information security are employed.*

	3.13.2[f]	*identified systems engineering principles that promote effective information security are employed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Security planning policy; procedures addressing system security plan development and implementation; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates; system and communications protection policy; procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the system; security architecture documentation; security requirements and specifications for the system; system design documentation; system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with responsibility for determining information system security requirements; personnel with information system design, development, implementation, and modification responsibilities; personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan; processes for applying security engineering principles in system specification, design, development, implementation, and modification; automated mechanisms supporting the application of security engineering principles in information system specification, design, development, implementation, and modification].	

3.13.3	**SECURITY REQUIREMENT** Separate user functionality from system management functionality.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.13.3[a]	*user functionality is identified.*
	3.13.3[b]	*system management functionality is identified.*
	3.13.3[c]	*user functionality is separated from system management functionality.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing application partitioning; system design documentation; system configuration settings and associated documentation; system security plan; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer]. **Test:** [*SELECT FROM:* Separation of user functionality from system management functionality].	

3.13.4	**SECURITY REQUIREMENT** Prevent unauthorized and unintended information transfer via shared system resources.	
	ASSESSMENT OBJECTIVE *Determine if unauthorized and unintended information transfer via shared system resources is prevented.*	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing application partitioning; system security plan; system design documentation; system	

	configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer]. **Test:** [*SELECT FROM:* Separation of user functionality from system management functionality].

3.13.5	**SECURITY REQUIREMENT** Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.13.5[a] *publicly accessible system components are identified.*
	3.13.5[b] *subnetworks for publicly accessible system components are physically or logically separated from internal networks.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; system security plan; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; system configuration settings and associated documentation; enterprise security architecture documentation; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer; personnel with boundary protection responsibilities]. **Test:** [*SELECT FROM:* Mechanisms implementing boundary protection capability].

3.13.6	**SECURITY REQUIREMENT** Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
	ASSESSMENT OBJECTIVE *Determine if:*
	3.13.6[a] *network communications traffic is denied by default.*
	3.13.6[b] *network communications traffic is allowed by exception.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer; personnel with boundary protection responsibilities]. **Test:** [*SELECT FROM:* Mechanisms implementing traffic management at managed interfaces].

3.13.7	**SECURITY REQUIREMENT** Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
	ASSESSMENT OBJECTIVE *Determine if remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; system security plan; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer; personnel with boundary protection responsibilities]. **Test**: [*SELECT FROM:* Mechanisms implementing boundary protection capability; mechanisms supporting or restricting non-remote connections].

3.13.8	**SECURITY REQUIREMENT** Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.13.8[a]	*cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.*
	3.13.8[b]	*alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified.*
	3.13.8[c]	*either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing transmission confidentiality and integrity; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer]. **Test:** [*SELECT FROM:* Cryptographic mechanisms or mechanisms supporting or implementing transmission confidentiality; organizational processes for defining and implementing alternative physical safeguards].	

3.13.9	**SECURITY REQUIREMENT** Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.13.9[a] *a period of inactivity to terminate network connections associated with communications sessions is defined.*
	3.13.9[b] *network connections associated with communications sessions are terminated at the end of the sessions.*
	3.13.9[c] *network connections associated with communications sessions are terminated after the defined period of inactivity.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing network disconnect; system design documentation; system security plan; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer]. **Test:** [*SELECT FROM:* Mechanisms supporting or implementing network disconnect capability].

3.13.10	**SECURITY REQUIREMENT** Establish and manage cryptographic keys for cryptography employed in organizational systems.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.13.10[a] *cryptographic keys are established whenever cryptography is employed.*
	3.13.10[b] *cryptographic keys are managed whenever cryptography is employed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing cryptographic key establishment and management; system security plan; system design documentation; cryptographic mechanisms; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel with responsibilities for cryptographic key establishment and management]. **Test:** [*SELECT FROM:* Mechanisms supporting or implementing cryptographic key establishment and management].

3.13.11	**SECURITY REQUIREMENT** Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
	ASSESSMENT OBJECTIVE *Determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS

	Examine: [*SELECT FROM:* System and communications protection policy; procedures addressing cryptographic protection; system security plan; system design documentation; system configuration settings and associated documentation; cryptographic module validation certificates; list of FIPS-validated cryptographic modules; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer; personnel with responsibilities for cryptographic protection]. **Test:** [*SELECT FROM:* Mechanisms supporting or implementing cryptographic protection].

3.13.12	**SECURITY REQUIREMENT** Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
	ASSESSMENT OBJECTIVE *Determine if:*
3.13.12[a]	*collaborative computing devices are identified.*
3.13.12[b]	*collaborative computing devices provide indication to users of devices in use.*
3.13.12[c]	*remote activation of collaborative computing devices is prohibited.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; system security plan; system design documentation; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer; personnel with responsibilities for managing collaborative computing devices]. **Test:** [*SELECT FROM:* Mechanisms supporting or implementing management of remote activation of collaborative computing devices; mechanisms providing an indication of use of collaborative computing devices].

3.13.13	**SECURITY REQUIREMENT** Control and monitor the use of mobile code.
	ASSESSMENT OBJECTIVE *Determine if:*
3.13.13[a]	*use of mobile code is controlled.*
3.13.13[b]	*use of mobile code is monitored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; system audit logs and records; system security plan; list of acceptable mobile code and mobile code technologies; list of unacceptable mobile code and mobile technologies; authorization records; system monitoring records; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel with responsibilities for managing mobile code].

	Test: [*SELECT FROM:* Organizational process for controlling, authorizing, monitoring, and restricting mobile code; mechanisms supporting or implementing the management of mobile code; mechanisms supporting or implementing the monitoring of mobile code].

3.13.14	**SECURITY REQUIREMENT** Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.13.14[a] *use of Voice over Internet Protocol (VoIP) technologies is controlled.*
	3.13.14[b] *use of Voice over Internet Protocol (VoIP) technologies is monitored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; VoIP implementation guidance; system security plan; system design documentation; system audit logs and records; system configuration settings and associated documentation; system monitoring records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel with responsibilities for managing VoIP]. **Test:** [*SELECT FROM:* Organizational process for authorizing, monitoring, and controlling VoIP; mechanisms supporting or implementing authorizing, monitoring, and controlling VoIP].

3.13.15	**SECURITY REQUIREMENT** Protect the authenticity of communications sessions.
	ASSESSMENT OBJECTIVE *Determine if the authenticity of communications sessions is protected.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing session authenticity; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Mechanisms supporting or implementing session authenticity].

3.13.16	**SECURITY REQUIREMENT** Protect the confidentiality of CUI at rest.
	ASSESSMENT OBJECTIVE *Determine if the confidentiality of CUI at rest is protected.*

	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing protection of information at rest; system security plan; system design documentation; list of information at rest requiring confidentiality protections; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer]. **Test:** [*SELECT FROM:* Mechanisms supporting or implementing confidentiality protections for information at rest].

3.14 SYSTEM AND INFORMATION INTEGRITY

3.14.1	**SECURITY REQUIREMENT** Identify, report, and correct system flaws in a timely manner.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.14.1[a]	*the time within which to identify system flaws is specified.*
	3.14.1[b]	*system flaws are identified within the specified time frame.*
	3.14.1[c]	*the time within which to report system flaws is specified.*
	3.14.1[d]	*system flaws are reported within the specified time frame.*
	3.14.1[e]	*the time within which to correct system flaws is specified.*
	3.14.1[f]	*system flaws are corrected within the specified time frame.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing flaw remediation; procedures addressing configuration management; system security plan; list of flaws and vulnerabilities potentially affecting the system; list of recent security flaw remediation actions performed on the system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct system flaws); test results from the installation of software and firmware updates to correct system flaws; installation/change control records for security-relevant software and firmware updates; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for flaw remediation; personnel with configuration management responsibility]. **Test:** [*SELECT FROM:* Organizational processes for identifying, reporting, and correcting system flaws; organizational process for installing software and firmware updates; mechanisms supporting or implementing reporting, and correcting system flaws; mechanisms supporting or implementing testing software and firmware updates].	

3.14.2	**SECURITY REQUIREMENT** Provide protection from malicious code at designated locations within organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.14.2[a]	*designated locations for malicious code protection are identified.*
	3.14.2[b]	*protection from malicious code at designated locations is provided.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; records of malicious code protection updates; malicious code protection mechanisms; system security plan; system configuration settings and associated documentation; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; scan results from malicious code protection mechanisms; system design documentation; system audit logs and records; other relevant documents or records].	

	Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility]. **Test:** [*SELECT FROM:* Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational process for addressing false positives and resulting potential impact; mechanisms supporting or implementing employing, updating, and configuring malicious code protection mechanisms; mechanisms supporting or implementing malicious code scanning and subsequent actions].

3.14.3	**SECURITY REQUIREMENT** Monitor system security alerts and advisories and take action in response.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.14.3[a] *response actions to system security alerts and advisories are identified.*
	3.14.3[b] *system security alerts and advisories are monitored.*
	3.14.3[c] *actions in response to system security alerts and advisories are taken.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing security alerts, advisories, and directives; system security plan; records of security alerts and advisories; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with security alert and advisory responsibilities; personnel implementing, operating, maintaining, and using the system; personnel, organizational elements, and external organizations to whom alerts, advisories, and directives are to be disseminated; system or network administrators; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives; mechanisms supporting or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives; mechanisms supporting or implementing security directives].

3.14.4	**SECURITY REQUIREMENT** Update malicious code protection mechanisms when new releases are available.
	ASSESSMENT OBJECTIVE *Determine if malicious code protection mechanisms are updated when new releases are available.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility].

	Test: [*SELECT FROM:* Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational process for addressing false positives and resulting potential impact; mechanisms supporting or implementing malicious code protection mechanisms (including updates and configurations); mechanisms supporting or implementing malicious code scanning and subsequent actions].

3.14.5	**SECURITY REQUIREMENT** Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.14.5[a] *the frequency for malicious code scans is defined.*
	3.14.5[b] *malicious code scans are performed with the defined frequency.*
	3.14.5[c] *real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility]. **Test:** [*SELECT FROM:* Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational process for addressing false positives and resulting potential impact; mechanisms supporting or implementing malicious code protection mechanisms (including updates and configurations); mechanisms supporting or implementing malicious code scanning and subsequent actions].

3.14.6	**SECURITY REQUIREMENT** Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.14.6[a] *the system is monitored to detect attacks and indicators of potential attacks.*
	3.14.6[b] *inbound communications traffic is monitored to detect attacks and indicators of potential attacks.*
	3.14.6[c] *outbound communications traffic is monitored to detect attacks and indicators of potential attacks.*

	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing system monitoring tools and techniques; continuous monitoring strategy; system and information integrity policy; procedures addressing system monitoring tools and techniques; facility diagram or layout; system security plan; system monitoring tools and techniques documentation; system design documentation; locations within system where monitoring devices are deployed; system protocols; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility monitoring the system; personnel with responsibility for the intrusion detection system]. **Test**: [*SELECT FROM:* Organizational processes for system monitoring; mechanisms supporting or implementing intrusion detection capability and system monitoring; mechanisms supporting or implementing system monitoring capability; organizational processes for intrusion detection and system monitoring; mechanisms supporting or implementing the monitoring of inbound and outbound communications traffic].

3.14.7	**SECURITY REQUIREMENT** Identify unauthorized use of organizational systems.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.14.7[a] *authorized use of the system is defined.*
	3.14.7[b] *unauthorized use of the system is identified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [SELECT FROM: Continuous monitoring strategy; system and information integrity policy; procedures addressing system monitoring tools and techniques; facility diagram/layout; system security plan; system design documentation; system monitoring tools and techniques documentation; locations within system where monitoring devices are deployed; system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for monitoring the system]. **Test:** [SELECT FROM: Organizational processes for system monitoring; mechanisms supporting or implementing system monitoring capability].

APPENDIX A

REFERENCES

LAWS, EXECUTIVE ORDERS, REGULATIONS, INSTRUCTIONS, STANDARDS, AND GUIDELINES[9]

LEGISLATION, EXECUTIVE ORDERS, AND REGULATIONS

1. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014. https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf
2. Executive Order 13526, *Classified National Security Information*, December 2009. https://www.archives.gov/isoo/policy-documents/cnsi-eo.html
3. Executive Order 13556, *Controlled Unclassified Information*, November 2010. https://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf
4. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 2013. https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
5. 32 CFR Part 2002, *Controlled Unclassified Information*, September 2016. https://www.gpo.gov/fdsys/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf

STANDARDS, GUIDELINES, INTERAGENCY REPORTS, AND INSTRUCTIONS

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. https://doi.org/10.6028/NIST.FIPS.199
2. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. https://doi.org/10.6028/NIST.FIPS.200
3. National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011. https://doi.org/10.6028/NIST.SP.800-39
4. National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013. https://doi.org/10.6028/NIST.SP.800-53r4
5. National Institute of Standards and Technology Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, December 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4

[9] References in this section without specific publication dates or revision numbers are assumed to refer to the most recent updates to those publications.

6. National Institute of Standards and Technology Special Publication 171, Revision 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, December 2016. https://doi.org/10.6028/NIST.SP.800-171r1

7. National Institute of Standards and Technology Special Publication 128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011. https://doi.org/10.6028/NIST.SP.800-128

8. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013, *Information technology -- Security techniques -- Information security management systems -- Requirements*, September 2013.

9. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002:2013, *Information technology -- Security techniques -- Code of practice for information security controls*, September 2013.

10. Committee on National Security Systems Instruction 4009, *National Information Assurance Glossary*, April 2015. https://www.cnss.gov

11. National Institute of Standards and Technology Internal Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, January 2017. https://doi.org/10.6028/NIST.IR.8062

OTHER RESOURCES

1. National Archives and Records Administration, *Controlled Unclassified Information Registry*. https://www.archives.gov/cui/registry/category-list

2. National Institute of Standards and Technology Handbook 162, *NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*, November 2017. https://doi.org/10.6028/NIST.HB.162

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-171. 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*.

agency	See *executive agency*.
assessment	See *Security Control Assessment*.
assessor	See *Security Control Assessor*.
audit log	A chronological record of system activities, including records of system accesses and operations performed in a given period.
audit record	An individual entry in an audit log related to an audited event.
authentication [FIPS 200, Adapted]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
baseline configuration	A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
blacklisting	A process used to identify software programs that are not authorized to execute on a system or prohibited Universal Resource Locators (URL)/websites.
confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
configuration management	A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
configuration settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.
controlled area	Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information or system.

controlled unclassified information [E.O. 13556]	Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.
CUI categories or subcategories [Title 32 CFR, Part 2002]	Those types of information for which laws, regulations, or governmentwide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI Executive Agent has approved and listed in the CUI Registry.
CUI Executive Agent [Title 32 CFR, Part 2002]	The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees federal agency actions to comply with Executive Order 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).
CUI program [Title 32 CFR, Part 2002]	The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI Registry.
CUI registry [Title 32 CFR, Part 2002]	The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.
environment of operation [NIST SP 800-37, Adapted]	The physical surroundings in which a system processes, stores, and transmits information.
executive agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 105; 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.
external system (or component)	A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
external system service	A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

external system service provider	A provider of external system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
external network	A network not controlled by the organization.
federal agency	See *executive agency*.
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. See *on behalf of (an agency)* for additional information.
FIPS-validated cryptography	A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See *NSA-Approved Cryptography*.
firmware	Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.
hardware	The physical components of a system. See *Software* and *Firmware*.
identifier	Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. A unique label used by a system to indicate a specific entity, object, or group.
impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system.
impact value	The assessed potential impact resulting from a compromise of the confidentiality of information (e.g., CUI) expressed as a value of low, moderate, or high.
incident [FIPS 200, Adapted]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

information flow control	Procedure to ensure that information transfers within a system are not made in violation of the security policy.
information resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
information security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
information system [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
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.
insider threat	The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.
integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
internal network	A network where establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or the cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.
least privilege	The principle that a system security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

local access	Access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.
malicious code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
media [FIPS 200]	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system.
mobile code	Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.
mobile device	A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable/removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-readers.
multifactor authentication	Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). See also *Authenticator*.
nonfederal organization	An entity that owns, operates, or maintains a nonfederal system.
nonfederal system	A system that does not meet the criteria for a federal system.
network	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
network access	Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).
nonlocal maintenance	Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.

on behalf of (an agency) [32 CFR Part 2002]	A situation that occurs when: (i) a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information; and (ii) those activities are not incidental to providing a service or product to the government.
organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure.
portable storage device	A system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain nonvolatile memory).
potential impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS Publication 199 low); (ii) a *serious* adverse effect (FIPS Publication 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
privileged account	A system account with authorizations of a privileged user.
privileged user	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
records	The recordings (automated and/or manual) 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 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 to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
remote maintenance	Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).
replay resistance	Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

risk [FIPS 200, Adapted]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems. Such risks reflect the potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation.
risk assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
sanitization	Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that form part of the enterprise's risk management approach.
security assessment	See *Security Control Assessment*.
security control [FIPS 199, Adapted]	A safeguard or countermeasure prescribed for a system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
security control assessment [CNSSI 4009, Adapted]	The testing or evaluation of security controls 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 a system or organization.
security functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational systems or the environments in which those systems operate.
security functions	The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

security relevance	Functions or mechanisms that are relied upon, directly or indirectly, to enforce a security policy that governs confidentiality, integrity, and availability protections.
situational awareness [CNSSI 4009]	Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.
split tunneling	The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing uncontrolled networks.
supplemental guidance	Statements used to provide additional explanatory information for security controls or security control enhancements.
system	See *Information System*.
system component [NIST SP 800-128, Adapted]	A discrete, identifiable information technology asset (hardware, software, firmware) that represents a building block of a system. System components include commercial information technology products.
system security plan	A document that describes how an organization meets the security requirements for a system or how an organization plans to meet the requirements. The system security plan describes the system boundary; the environment in which the system operates; the relationships with or connections to other systems; and how the security requirements are implemented.
system service	A capability provided by a system that facilitates information processing, storage, or transmission.
threat [CNSSI 4009, Adapted]	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
user [CNSSI 4009, Adapted]	Individual, or (system) process acting on behalf of an individual, authorized to access a system.
whitelisting	A process used to identify software programs that are authorized to execute on a system or authorized Universal Resource Locators (URL)/websites.
wireless technology	Technology that permits the transfer of information between separated points without physical connection.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CUI	Controlled Unclassified Information
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISOO	Information Security Oversight Office
ITL	Information Technology Laboratory
NARA	National Archives and Records Administration
NFO	Nonfederal Organization
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SP	Special Publication
SSP	System Security Plan

APPENDIX D

ASSESSMENT METHODS

ASSESSMENT METHOD DEFINITIONS, APPLICABLE OBJECTS, AND ATTRIBUTES

This appendix defines three assessment methods that can be used to assess the CUI security requirements in NIST Special Publication 800-171: *examine*, *interview*, and *test*. Included in the definition of each assessment method are types of objects to which the method can be applied. The application of each method is described in terms of the attributes of *depth* and *coverage*, progressing from *basic* to *focused* to *comprehensive*. The attribute values correlate to the assurance requirements specified by the organization.

The depth attribute addresses the rigor and level of detail of the assessment. For the depth attribute, the *focused* attribute value includes and builds upon the assessment rigor and level of detail defined for the *basic* attribute value; the *comprehensive* attribute value includes and builds upon the assessment rigor and level of detail defined for the *focused* attribute value.

The coverage attribute addresses the scope or breadth of the assessment. For the coverage attribute, the *focused* attribute value includes and builds upon the number and type of assessment objects defined for the *basic* attribute value; the *comprehensive* attribute value includes and builds upon the number and type of assessment objects defined for the *focused* attribute value.

Tables D-1 through D-3 provide complete descriptions of the examine, interview, and test assessment methods. The use of **bolded text** in the assessment method description indicates the content that was added to and appears for the first time, in the description indicating greater rigor and level of detail for the attribute value.

TABLE D-1: EXAMINE ASSESSMENT METHOD

Method	**EXAMINE** 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 are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.		
Objects	***Specifications***	Examples: policies, plans, procedures, system requirements, designs.	
	Mechanisms	Examples: functionality implemented in hardware, software, firmware.	
	Activities	Examples: system operations, administration, management, exercises.	
Attributes	***Depth***	Addresses the rigor of and level of detail in the *examination* process.	
		Basic	Examination that consists of high-level reviews, checks, observations, or inspections of the assessment object. This type of examination is conducted using a limited body of evidence or documentation. Examples include: functional-level descriptions for mechanisms; high-level process descriptions for activities; and documents for specifications. Basic examinations provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors.
		Focused	Examination that consists of high-level reviews, checks, observations, or inspections **and more in-depth studies and analyses** of the assessment object. This type of examination is conducted using a **substantial** body of evidence or documentation. Examples include: functional-level descriptions **and where appropriate and available, high-level design information** for mechanisms; high-level process descriptions **and implementation procedures** for activities; and documents **and related documents** for specifications. **Focused** examinations provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors **and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended**.
		Comprehensive	Examination that consists of high-level reviews, checks, observations, or inspections and more in-depth, **detailed, and thorough** studies and analyses of the assessment object. This type of examination is conducted using an **extensive** body of evidence or documentation. Examples include: functional-level descriptions and where appropriate and available, high-level design information, **low-level design information, and implementation information** for mechanisms; high-level process descriptions and **detailed** implementation procedures for activities; and documents and related documents for specifications.[10] **Comprehensive** examinations provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the safeguards are implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards**.

[10] While additional documentation is likely for mechanisms when moving from basic to focused to comprehensive examinations, the documentation associated with specifications and activities may be the same or similar for focused and comprehensive examinations, with the rigor of the examinations of these documents being increased at the comprehensive level.

	Coverage	Addresses the scope or breadth of the examination process and includes the types of assessment objects to be examined; the number of objects to be examined by type; and specific objects to be examined.[11]	
		Basic	Examination that uses a representative sample of assessment objects (by type and number within type) to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors.
		Focused	Examination that uses a representative sample of assessment objects (by type and number within type) **and other specific assessment objects deemed particularly important to achieving the assessment objective** to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors **and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended**.
		Comprehensive	Examination that uses a **sufficiently large** sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the safeguards are implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards**.
	DISCUSSION 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 training records; reviewing audit records; observing incident response activities; studying technical manuals and user/administrator guides; checking, studying, or observing the operation of an information technology mechanism in the system hardware or software; or checking, studying, or observing physical security measures related to the operation of a system.		

[11] The organization, considering a variety of factors (e.g., available resources, importance of the assessment, the organization's overall assessment goals and objectives), confers with assessors and provides direction on the type, number, and specific objects to be examined for the attribute value described.

TABLE D-2: INTERVIEW ASSESSMENT METHOD

Method	**INTERVIEW** The process of conducting discussions with individuals or groups of individuals in an organization to facilitate understanding, achieve clarification, or lead to the location of evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.		
Objects	***Individuals or Groups***	Examples: Personnel with risk assessment responsibilities; personnel with information security responsibilities; system or network administrators; personnel with account management responsibilities.	
Attributes	***Depth***	Addresses the rigor of and level of detail in the *interview* process.	
		Basic	Interview that consists of broad-based, high-level discussions with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions. Basic interviews provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors.
		Focused	Interview that consists of broad-based, high-level discussions **and more in-depth discussions in specific areas** with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions **and more in-depth questions in specific areas where responses indicate a need for more in-depth investigation**. **Focused** interviews provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors **and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended**.
		Comprehensive	Interview that consists of broad-based, high-level discussions and more in-depth, **probing** discussions in specific areas with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions and more in-depth, **probing** questions in specific areas where responses indicate a need for more in-depth investigation. **Comprehensive** interviews provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the safeguards are implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards**.
	Coverage	Addresses the scope or breadth of the interview process and includes the types of individuals to be interviewed by role and responsibility; the number of individuals to be interviewed by type; and specific individuals to be interviewed.[12]	
		Basic	Interview that uses a representative sample of individuals in organizational roles to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors.

[12] The organization, considering a variety of factors (e.g., available resources, importance of the assessment, the organization's overall assessment goals and objectives), confers with assessors and provides direction on the type, number, and specific individuals to be interviewed for the attribute value described.

		Focused	Interview that uses a representative sample of individuals in organizational roles **and other specific individuals deemed particularly important to achieving the assessment objective** to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors **and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended**.
		Comprehensive	Interview that uses a **sufficiently large** sample of individuals in organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the safeguards are implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards**.
	DISCUSSION Typical assessor actions may include, for example, interviewing chief executive officers, chief information officers, senior information security officers, information owners, system and mission owners, system security officers, system security managers, personnel officers, human resource managers, network and system administrators, facilities managers, training officers, physical security officers, system operators, site managers, and users.		

TABLE D-3: TEST ASSESSMENT METHOD

Method	**TEST** The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.[13]		
Objects	***Mechanisms***	Examples: hardware, software, firmware.	
	Activities	Examples: system operations, administration, management; exercises.	
Attributes	***Depth***	Addresses the types of testing to be conducted.	
		Basic	Test methodology (also known as *black box* testing) that assumes no knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification for mechanisms and a high-level process description for activities. Basic testing provides a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors.
		Focused	Test methodology (also known as *gray box* testing) that assumes **some** knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification **and limited system architectural information (e.g., high-level design)** for mechanisms and a high-level process description **and high-level description of integration into the operational environment** for activities. Focused testing provides a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors **and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended**.
		Comprehensive	Test methodology (also known as *white box* testing) that assumes **explicit and substantial** knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification, **extensive** system architectural information (e.g., high-level design, **low-level design) and implementation representation (e.g., source code, schematics)** for mechanisms and a high-level process description and **detailed** description of integration into the operational environment for activities. Comprehensive testing provides a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the safeguards are implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards**.
	Coverage	Addresses the scope or breadth of the testing process and includes the types of assessment objects to be tested; the number of objects to be tested by type; and specific objects to be tested.	

[13] Testing is typically used to determine if mechanisms or activities meet a set of predefined specifications. Testing can also be performed to determine characteristics of a security or privacy control that are not commonly associated with predefined specifications, with an example of such testing being penetration testing.

		Basic	Testing that uses a representative sample of assessment objects by type and number within type, to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors.
		Focused	Testing that uses a representative sample of assessment objects by type and number within type, **and other specific assessment objects deemed particularly important to achieving the assessment objective** to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors **and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended**.
		Comprehensive	Testing that uses a **sufficiently large** sample of assessment objects by type and number within type, and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the safeguards are implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards**.
	DISCUSSION Typical assessor actions may include, for example: testing access control, identification and authentication, and audit mechanisms; testing security configuration settings; testing physical access control devices; conducting penetration testing of key system components; testing system backup operations; testing incident response capability; and exercising vulnerability scanning capability.		