Draft NIST Special Publication 800-171A

Assessing Security Requirements for Controlled Unclassified Information

RON ROSS
KELLEY DEMPSEY
VICTORIA PILLITTERI

This publication contains procedures to assess the CUI security requirements in *NIST Special Publication 800-171*. The content in this publication is derived from *NIST Special Publication 800-53A*, which provides assessment procedures to determine the effectiveness of the security controls in *NIST Special Publication 800-53*. Organizations are encouraged to consult NIST Special Publication 800-53A when developing their plans to assess CUI security requirements.

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

Draft 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

February
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, **133 pages** (February 2018)
CODEN: NSPUE2

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 **http://csrc.nist.gov/publications**.

Public comment period: February 20 through March 23, 2018

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; Nonfederal Organization; Nonfederal System; Security Assessment; Security Control.

Acknowledgements

The authors gratefully acknowledge and appreciate the contributions from Jon Boyens, Devin Casey, Ned Goren, Gary Guissanie, Jody Jacobs, Vicki Michetti, Mark Riddle, Mary Thomas, Matt Scholl, Gary Stoneburner, Patricia Toth, and Patrick Viscuso whose thoughtful and constructive comments improved the overall 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.

Notes to Reviewers

This publication is intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the CUI security requirements defined in Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. This objective is accomplished by:

- Providing flexible and tailorable assessment procedures for the CUI security requirements;
- Defining assessment objectives to help guide and inform the assessment;
- Specifying assessment methods that can be used to generate evidence and produce findings and results;
- Describing a set of assessment objects to which the methods can be applied;
- Facilitating different levels of assurance in security assessments by varying the scope and rigor of the assessment through selectable depth and coverage attributes; and
- Providing a discussion section for each CUI security requirement to explain and interpret the requirement and to facilitate more effective assessments of the requirement.

There is no expectation that all assessment methods and assessment objects will be selected for each assessment procedure—rather, the procedures should be used by organizations as a starting point for developing assessment plans and approaches that can produce the level of evidence needed for risk-based decisions or to determine compliance to the CUI security requirements.

We are seeking your feedback on the assessment procedures including the assessment objectives, determination statements, and the usefulness of the assessment objects and methods provided for each procedure. We are also interested in the need to provide additional clarifying language to promote assessor understanding.

One significant change to the final draft is the elimination of the mapping tables in Appendix E. The tables have been removed from this publication as the same information can be found in NIST Special Publication 800-171. Providing this information in one publication will help ensure greater consistency over time as the tables are updated. Two new appendixes have been added to the publication including a *Glossary* appendix and an *Acronyms* appendix. In addition, the title of the *Supplemental Guidance* appendix has been changed to *Discussion* to eliminate any potential misinterpretation or confusion that the information in that section contains any implied, derived, or extended CUI security requirements. NIST plans to move the *Discussion* appendix to Special Publication 800-171 after the final public comment period as it is a more appropriate publication for such information. Finally, we have received many requests to include templates for system security plans in this publication. While not included in the final draft, we do plan to post the sample templates on the CSRC website.

Your feedback on this draft publication is important to us. We appreciate each contribution from our reviewers. The very insightful comments from both the public and private sectors, nationally and internationally, continue to help shape the final publication to ensure that it meets the needs and expectations of our customers.

– **RON ROSS**
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

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 identify 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 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 widely recognized that the communities of interest affected by the CUI security requirements is broad and diverse, other supporting assessment guidance may be developed for those communities. For example, NIST's Manufacturing Extension Partnership 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

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 disciplined and structured process for identifying the different types of information that are routinely used by federal agencies. On November 4, 2010, the President signed Executive Order 13556, *Controlled Unclassified Information*. The Executive Order 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*, went into effect on November 14, 2016. The CUI Executive Agent (EA) is the National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees Federal agency actions to comply with the Order. Only federal information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI. NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, specifies the security requirements that must be satisfied to ensure the confidentiality of CUI.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide a set of procedures for assessing the CUI security requirements in NIST Special Publication 800-171. The security requirements have been defined to protect the *confidentiality* of CUI:

- When such information is resident in a nonfederal system or organization;
- When the nonfederal organization is *not* collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency;[2] and
- Where there are no specific safeguarding requirements for protecting the confidentiality of CUI that is prescribed by the authorizing law, regulation, or governmentwide policy for the category or subcategory listed in the CUI Registry.

The CUI security requirements apply *only* to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.[3] Accordingly, the assessment procedures in this publication are intended to be applied within that same scope. The CUI security requirements are intended for use by federal agencies in appropriate contractual

[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 Government-wide 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] Nonfederal organizations that collect or maintain information *on behalf of* a federal agency or that use or operate a system *on behalf of* an agency, must comply with the requirements in FISMA, including the requirements in FIPS Publication 200 and the security controls in NIST Special Publication 800-53 (See 44 USC 3554(a)(1)(A)).

[3] System *components* include, for example: mainframes, workstations, servers; input and output devices; network components; operating systems; virtual machines; and applications.

vehicles or other agreements established between those agencies and nonfederal organizations. Compliance with the requirements is addressed in CUI guidance and the CUI Federal Acquisition Regulation (FAR)[4] 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. The information gathered and 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-related weaknesses and deficiencies in its systems and in the environments in which those systems operate;
- Prioritize risk mitigation decisions and associated risk mitigation activities;
- Confirm that identified security-related weaknesses and deficiencies in the system and in the environment of operation have been addressed; and
- Support monitoring activities and information security situational awareness.

The assessment procedures in this publication promote a consistent level of security and offer the needed flexibility to customize assessments based on organizational policies and requirements, known threat and vulnerability information, operational considerations, system and platform dependencies, and tolerance for risk.[5]

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.

* The term *organizational system* has a specific meaning regarding the scope of applicability for the CUI security requirements—that is, the requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

[4] 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.

[5] In this publication, 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.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse group of system, information security, and privacy[6] professionals including:

- Individuals with system development responsibilities (e.g., program managers, system developers, system owners, systems integrators, system security engineers);
- Individuals with information security assessment and monitoring responsibilities (e.g., system evaluators, assessors, independent verifiers/validators, auditors, analysts, system owners);
- Individuals with 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
- Individuals with 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 a description of assessment procedures, methods, and objects; and explains the concept of assurance cases that can be created using evidence produced during assessments.
- **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; a description of the assessment methods used in assessment procedures; and a discussion of the individual security requirements to facilitate more effective implementation and assessments.

[6] 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 TWO

THE FUNDAMENTALS

BASIC CONCEPTS ASSOCIATED WITH ASSESSMENTS OF CUI SECURITY REQUIREMENTS

The CUI security requirements in NIST Special Publication 800-171 are organized into fourteen families.[7] 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 provided in Chapter Three are grouped by these family designations to help ensure completeness and consistency of assessments of CUI requirements.

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

[7] The families are closely aligned with the minimum-security requirements in FIPS Publication 200 and the security control families in NIST Special Publication 800-53. The contingency planning, system and services acquisition, and planning families are not included due to the tailoring criteria described in NIST Special Publication 800-171. Three exceptions include: a requirement to protect the confidentiality of system backups (derived from CP-9); a requirement to develop and implement a system security plan (derived from PL-2); and a requirement to implement system security engineering principles (derived from SA-8). For convenience, these requirements are included with the CUI media protection, security assessment, and system and communications protection requirements families, respectively.

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 one or more of the assessment objects (i.e., specifications, mechanisms, or 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 once again, facilitate understanding, achieve clarification, or obtain evidence. The test method is the process of exercising one or more assessment objects (i.e., activities or 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 help 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 that may be needed for some organizations and systems. A complete description of assessment methods and objects is provided in Appendix D.[8] Figure 1 illustrates an example of an assessment procedure for CUI security requirement 3.1.4 from NIST Special Publication 800-171.

3.1.4	**SECURITY REQUIREMENT** Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
	ASSESSMENT OBJECTIVE *Determine if, for an organizational system that processes, stores, or transmits CUI:*	
	3.1.4[a]	*the duties of individuals requiring separation to reduce the risk of malevolent activity are defined.*
	3.1.4[b]	*organization-defined duties of individuals requiring separation are separated.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing divisions of responsibility and separation of duties; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.1.4	

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

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

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.

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 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.

2.2 ASSURANCE CASES

Building an effective assurance case[9] 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. Assessors gather evidence during the assessment process to allow designated officials[10] to make objective determinations about organizational compliance to the CUI security requirements. The assessment evidence needed to make such determinations can be obtained from 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.[11] 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.

[9] An assurance case is a body of evidence organized into an argument demonstrating that some claim about a system holds (i.e., is assured). For assessments conducted using the procedures in this publication, that claim is *compliance* with the security requirements specified in NIST Special Publication 800-171.

[10] 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.

[11] 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 Standards (FIPS) 140.

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, assessors, auditors, system owners, and 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, if available. 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 security plan. System assessments can be used to compile and evaluate the evidence needed by organizational officials 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.

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. A 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 non-compliance. 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 that a certain number of assessment methods or objects must be selected to determine compliance to the CUI security requirements. Moreover, the list of potential assessment objects should not be viewed as required artifacts needed to determine compliance to the requirements. There is flexibility in determining which assessment methods and assessment objects are deemed to be the most useful in obtaining the evidence needed to support claims of compliance.

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 choose to define subcategories of findings indicating the severity or criticality of the weaknesses or deficiencies discovered and the potential adverse effects on organizations. Defining such subcategories can help to establish priorities for needed risk mitigation actions. Organizations may also choose to employ a more granular approach to findings by introducing a *partially satisfied* category for assessments.

THE MEANING OF ORGANIZATIONAL SYSTEM

The term *organizational system* is used in many of the CUI security requirements in NIST Special Publication 800-171 and in the associated assessment procedures in this publication. This term has a specific meaning regarding the scope of applicability for the CUI security requirements—that is, the security requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. The appropriate scoping for the security requirements is an important factor in determining protection-related investment decisions and managing security risk for nonfederal organizations that have the responsibility of safeguarding CUI. Moreover, it also limits the scope of security assessments for CUI security requirements.

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 (including 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; 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 records; system audit logs and records; other relevant documents or records; list of devices and other systems authorized to connect to organizational systems]. **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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.1.1	

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; security plan; system design documentation; list of approved authorizations (user privileges) including remote access authorizations; system configuration settings and associated documentation; system audit logs and records; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.2

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 systems 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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.1.3	

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 to reduce the risk of malevolent activity are defined.*
	3.1.4[b]	*organization-defined duties of individuals requiring separation are separated.*
	3.1.4[c]	*separate accounts for individuals whose duties and accesses must be separated to reduce the risk of malevolent activity or collusion are established.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing divisions of responsibility and separation of duties; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.4

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; 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; other relevant documents or records; procedures addressing least privilege; list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; list of system-generated privileged accounts; list of system administration personnel]. **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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.5

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.6

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.7

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.8

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:* Access control policy; 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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.9

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.10

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.11

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; security plan; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.12

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.1.13	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.1.14	

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.15

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); 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.16

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 encryption.*
	3.1.17[b] *wireless access to the system is protected using authentication.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; system design documentation; procedures addressing wireless implementation and usage (including restrictions); 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.17

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] *the connection of mobile devices is 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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.18

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.1.19

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]	*use of external systems is identified.*
	3.1.20[c]	*connections to external systems are verified.*
	3.1.20[d]	*use of external systems is verified.*
	3.1.20[e]	*connections to external systems are controlled/limited.*
	3.1.20[f]	*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; security plan; list of types of applications accessible from external systems; system configuration settings and associated documentation; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.1.20	

3.1.21	**SECURITY REQUIREMENT** Limit use of organizational portable storage devices on external systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.21[a]	*use of organizational portable storage devices containing CUI on external systems is identified and documented.*
	3.1.21[b]	*limits on the use of organizational portable storage devices containing CUI on external systems are defined.*
	3.1.21[c]	*use of organizational 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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.1.21	

3.1.22	**SECURITY REQUIREMENT** Control CUI posted or processed on publicly accessible systems.
	ASSESSMENT OBJECTIVE *Determine if CUI posted or processed on publicly accessible systems is controlled.*

	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 in in place prior to posting of any content to publicly accessible systems.*
	3.1.22[d]	*content on publicly accessible information 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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.1.22	

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; 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]. **Test**: [*SELECT FROM:* Mechanisms managing security awareness training; mechanisms managing role-based security training].	
	DISCUSSION ON SECURITY REQUIREMENT 3.2.1	

3.2.2	**SECURITY REQUIREMENT** Ensure that organizational personnel are adequately 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; 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]. **Test**: [*SELECT FROM:* Mechanisms managing role-based security training].
	DISCUSSION ON SECURITY REQUIREMENT 3.2.2

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.2.3

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; security plan; system design documentation; system configuration settings and associated documentation; 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; system or network administrators]. **Test**: [*SELECT FROM:* Mechanisms implementing system audit logging].	
	DISCUSSION ON SECURITY REQUIREMENT 3.3.1	

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; security plan; system design documentation; system configuration settings and associated documentation; 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].	

	DISCUSSION ON SECURITY REQUIREMENT 3.3.2

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.3.3

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.3.4

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; security plan; system design documentation; system configuration settings and associated documentation; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.3.5

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.3.6

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.3.7	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.3.8	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.3.9	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.4.1	

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; procedures addressing configuration settings for the system; configuration management plan; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.4.2

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.4.3

3.4.4	**SECURITY REQUIREMENT** Analyze the security impact of changes prior to implementation.
	ASSESSMENT OBJECTIVE *Determine if the security impact of changes to each organizational system is analyzed prior to implementation.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing security impact analysis for changes to the system; configuration management plan; security impact analysis documentation; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.4.4

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.4.5

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.4.6	

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; security plan; system design documentation; system configuration settings and associated documentation; specifications for preventing software program execution; security configuration	

	checklists; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.4.7

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.4.8

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.4.9	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.5.1	

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; procedures addressing authenticator management; security plan; system design documentation; system configuration settings and associated documentation; list of system authenticator types; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.5.2	

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.5.3

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 all 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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.5.4

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.5.5

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.5.6

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.5.7	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.5.8	

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.5.9

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.5.10

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.5.11

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.6.1	

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.6.2

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; security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with incident response testing responsibilities; personnel with information security responsibilities].
	DISCUSSION ON SECURITY REQUIREMENT 3.6.3

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.7.1

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.7.2	

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.7.3

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.7.4

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 required 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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.7.5

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.7.6

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 access restrictions; access control policy and procedures; physical and environmental protection policy and procedures; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.8.1	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.8.2	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.8.3	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.8.4	

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.8.5

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.8.6

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 containing CUI is controlled.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; system use policy; procedures addressing media usage restrictions; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.8.7

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; 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 prohibiting use of media on systems or system components].
	DISCUSSION ON SECURITY REQUIREMENT 3.8.8

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; security plan; backup storage location(s); 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.8.9

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.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing personnel screening; records of screened personnel; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.9.1

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 authorization 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.9.2	

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]	*for a facility that contains CUI, authorized individuals allowed physical access are identified.*
	3.10.1[b]	*physical access to an organizational system that processes, stores, or transmits CUI is limited to authorized individuals.*
	3.10.1[c]	*physical access to equipment that processes, stores, or transmits CUI is limited to authorized individuals.*
	3.10.1[d]	*physical access to operating environments where CUI is processed, stored, or transmitted is limited to authorized individuals.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.10.1	

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 that system resides is protected.*
	3.10.2[b]	*the support infrastructure for that system is protected.*
	3.10.2[c]	*the physical facility where that system resides is monitored.*
	3.10.2[d]	*the support infrastructure for that system is monitored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access monitoring; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.10.2

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.10.3

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.10.4

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.10.5

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.10.6

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.11.1	

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 an organizational system and its applications that process, store, or transmit CUI is defined.*
	3.11.2[b]	*vulnerability scans are performed in an organizational system that processes, stores, or transmits CUI with the defined frequency.*
	3.11.2[c]	*vulnerability scans are performed in an application that contains CUI with the defined frequency.*
	3.11.2[d]	*vulnerability scans are performed in an organizational system that processes, stores, or transmits CUI when new vulnerabilities are identified.*
	3.11.2[e]	*vulnerability scans are performed in an application that contains CUI when new vulnerabilities are identified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.11.2

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.11.3

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.12.1	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.12.2	

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 security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan; records of security plan reviews and updates; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with security planning and plan implementation responsibilities; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for security plan development, review, update, and approval; mechanisms supporting the security plan].
	DISCUSSION ON SECURITY REQUIREMENT 3.12.3

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]	*how security requirements are implemented is described and documented in the system security plan.*
	3.12.4[e]	*the relationship with or connection to other systems is described and documented in the system security plan.*
	3.12.4[f]	*the frequency to update the system security plan is defined.*
	3.12.4[g]	*system security plan is updated with the defined frequency.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* Security planning policy; procedures addressing security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan; records of security plan reviews and updates; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with security planning and plan implementation responsibilities; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for security plan development, review, update, and approval; mechanisms supporting the security plan].	
	DISCUSSION ON SECURITY REQUIREMENT 3.12.4	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.13.1	

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 security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan; records of security plan reviews and updates; other relevant documents or records]. **Interview:** [*SELECT FROM:* Personnel with security planning and plan implementation responsibilities; personnel with information security responsibilities]. **Test:** [*SELECT FROM:* Organizational processes for security plan development, review, update, and approval; mechanisms supporting the system security plan].	
	DISCUSSION ON SECURITY REQUIREMENT 3.13.2	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.13.3	

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; 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].	

	DISCUSSION ON SECURITY REQUIREMENT 3.13.4

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.13.5

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.13.6

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.13.7

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.13.8	

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.13.9

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.13.10

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.13.11

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; 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 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.13.12	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.13.13	

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; security plan; system design documentation; system configuration settings and associated documentation; 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 VoIP]. **Test:** [*SELECT FROM:* Organizational process for authorizing, monitoring, and controlling VoIP; mechanisms supporting or implementing authorizing, monitoring, and controlling VoIP].	
	DISCUSSION ON SECURITY REQUIREMENT 3.13.14	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.13.15	

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.13.16

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.14.1	

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; security plan; system design documentation; 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 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.14.2

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.14.3

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.14.4

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; 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].
	DISCUSSION ON SECURITY REQUIREMENT 3.14.5

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; security plan; system design documentation; system monitoring tools and techniques 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.14.6	

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; 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].	
	DISCUSSION ON SECURITY REQUIREMENT 3.14.7	

APPENDIX A

REFERENCES

LAWS, EXECUTIVE ORDERS, REGULATIONS, INSTRUCTIONS, STANDARDS, AND GUIDELINES[12]

LEGISLATION, EXECUTIVE ORDERS, AND REGULATIONS

1. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014. http://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf
2. Executive Order 13556, *Controlled Unclassified Information*, November 2010. http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf
3. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
4. 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
5. Executive Order, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 2017. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

STANDARDS, GUIDELINES, INTERAGENCY REPORTS, AND INSTRUCTIONS

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199 (as amended), *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 (as amended), *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 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013. https://doi.org/10.6028/NIST.SP.800-53Ar4
4. 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

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

5. 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

6. National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, February 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

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

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

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

10. 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.
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 security architecture should be 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 should 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.
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. In particular, the system security plan describes the system boundary; the environment in which the system operates; how the security requirements are implemented; and the relationships with or connections to other systems.
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.[13] **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**.

[13] 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.[14]	
		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.		

[14] 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.[15]	
		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.

[15] 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.[16]			
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.		

[16] 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.		

APPENDIX E

DISCUSSION

IMPLEMENTING AND ASSESSING CUI SECURITY REQUIREMENTS

Tables E-1 through E-14 provide discussion intended to facilitate implementing and assessing the CUI security requirements in NIST Special Publication 800-171. This information is derived primarily from the security controls and supplemental guidance in NIST Special Publication 800-53, and is provided to give assessors a better understanding of the mechanisms and procedures used to implement the safeguards employed to protect CUI. The discussion is *not* intended to extend the security requirements or the scope of the assessments of those requirements.

TABLE E-1: DISCUSSION ON ACCESS CONTROL REQUIREMENTS

3.1.1	**SECURITY REQUIREMENT** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	DISCUSSION Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without a demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: when shared/group, emergency, or temporary accounts are no longer required, or when individuals are transferred or terminated. Some types of system accounts may require specialized training. This requirement focuses on account management, both system and application. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2.
3.1.2	**SECURITY REQUIREMENT** Limit system access to the types of transactions and functions that authorized users are permitted to execute.
	DISCUSSION System account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, and temporary. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example: restrictions on time-of-day, day-of-

	week, and point-of-origin. In defining other account attributes, organizations may consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission or business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect system availability.
3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.
	DISCUSSION Information flow control regulates where information can travel within a system and between systems (as opposed to who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example: keeping export-controlled information from being transmitted in the clear to the Internet; blocking outside traffic that claims to be from within the organization; restricting requests to the Internet that are not from the internal web proxy server; and limiting information transfers between organizations based on data structures and content. Transferring information between systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: prohibiting information transfers between interconnected systems (i.e., allowing access only); employing hardware mechanisms to enforce one-way information flows; and implementing trustworthy regrading mechanisms to reassign security attributes and security labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within systems and between interconnected systems. Flow control is based on characteristics of the information or the information path. Enforcement occurs in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.
3.1.4	**SECURITY REQUIREMENT** Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
	DISCUSSION Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and ensuring that security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.
3.1.5	**SECURITY REQUIREMENT** Employ the principle of least privilege, including for specific security functions and privileged accounts.

	DISCUSSION Organizations employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational systems. Security functions include, for example, establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations (i.e., permissions, privileges). Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information or functions. Organizations may differentiate in the application of this requirement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.
3.1.6	**SECURITY REQUIREMENT** Use non-privileged accounts or roles when accessing nonsecurity functions.
	DISCUSSION This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.
3.1.7	**SECURITY REQUIREMENT** Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
	DISCUSSION Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat. Privileged functions include, for example, establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and intrusion prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. Note that this requirement represents a condition to be achieved by the definition of authorized privileges in 3.1.2.
3.1.8	**SECURITY REQUIREMENT** Limit unsuccessful logon attempts.
	DISCUSSION This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the organization. If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components. Responses to

	unsuccessful logon attempts may be implemented at the operating system and the application levels.
3.1.9	**SECURITY REQUIREMENT** Provide privacy and security notices consistent with applicable CUI rules.
	DISCUSSION System use notifications can be implemented using messages or warning banners displayed before individuals log in to organizational systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Based on an assessment of risk, organizations consider whether a secondary system use notification is needed to access applications or other system resources after the initial network logon. Where necessary, posters or other printed materials may be used in lieu of an automated system banner. Organizations should consult with the Office of the General Counsel for legal review and approval of warning banner content.
3.1.10	**SECURITY REQUIREMENT** Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
	DISCUSSION Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of the system, for example, if organizations require users to log out at the end of the workday. Pattern-hiding displays can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey controlled unclassified information.
3.1.11	**SECURITY REQUIREMENT** Terminate (automatically) a user session after a defined condition.
	DISCUSSION This requirement addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., disconnecting from the network). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on system use.
3.1.12	**SECURITY REQUIREMENT** Monitor and control remote access sessions.
	DISCUSSION Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and help to ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

	Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example: dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate safeguards (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code. NIST Special Publications 800-46, 800-77, and 800-113 provide guidance on secure remote access and virtual private networks.
3.1.13	**SECURITY REQUIREMENT** Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
	DISCUSSION Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. See NIST Cryptographic Standards; NIST Cryptographic Module Validation Program; NIST Cryptographic Algorithm Validation Program; NSA Cryptographic Standards.
3.1.14	**SECURITY REQUIREMENT** Route remote access via managed access control points.
	DISCUSSION Routing all remote access through managed access control points enhances explicit, organizational control over such connections, reducing the susceptibility to unauthorized access to organizational systems resulting in the unauthorized disclosure of CUI.
3.1.15	**SECURITY REQUIREMENT** Authorize remote execution of privileged commands and remote access to security-relevant information.
	DISCUSSION A privileged command is a human-initiated (interactively or via a process operating on behalf of the human) command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. Security-relevant information is any information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Privileged commands give individuals the ability to execute sensitive, security-critical, or security-relevant system functions. Controlling such access from remote locations helps to ensure that unauthorized individuals are not able to execute such commands freely with the potential to do serious or catastrophic damage to organizational systems. Note that the ability to affect the integrity of the system is considered security-relevant as that could enable the means to by-pass security functions although not directly impacting the function itself.
3.1.16	**SECURITY REQUIREMENT** Authorize wireless access prior to allowing such connections.
	DISCUSSION Establishing usage restrictions and configuration/connection requirements for wireless access to the system provides criteria for organizations to support wireless access authorization decisions. Such restrictions and requirements reduce the susceptibility to unauthorized access to the system through wireless technologies. Wireless networks use authentication protocols which provide

	credential protection and mutual authentication. NIST Special Publications 800-48 and 800-97 provide guidance on secure wireless networks.
3.1.17	**SECURITY REQUIREMENT** Protect wireless access using authentication and encryption.
	DISCUSSION Organizations can authenticate individuals and devices to help protect wireless access to the system. Special attention should be given to the wide variety of devices that are part of the Internet of Things with potential wireless access to organizational systems. See NIST Cryptographic Standards.
3.1.18	**SECURITY REQUIREMENT** Control connection of mobile devices.
	DISCUSSION A mobile device is a 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 or removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, or built-in features for synchronizing local data with remote locations. Examples of mobile devices include smart phones, e-readers, and tablets. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different types of devices. Usage restrictions and implementation guidance for mobile devices include, for example: configuration management; device identification and authentication; implementation of mandatory protective software (e.g., malicious code detection, firewall); scanning devices for malicious code; updating virus protection software; scanning for critical software updates and patches; conducting primary operating system (and possibly other resident software) integrity checks; and disabling unnecessary hardware (e.g., wireless, infrared). The need to provide adequate security for mobile devices goes beyond this requirement. Many safeguards for mobile devices are reflected in other CUI security requirements. NIST Special Publication 800-124 provides guidance on mobile device security.
3.1.19	**SECURITY REQUIREMENT** Encrypt CUI on mobile devices and mobile computing platforms.
	DISCUSSION Organizations can use full-device encryption or container-based encryption to protect the confidentiality of CUI on mobile devices and computing platforms. Container-based encryption provides a more fine-grained approach to the encryption of data and information including, for example, encrypting selected data structures such as files, records, or fields. See NIST Cryptographic Standards.
3.1.20	**SECURITY REQUIREMENT** Verify and control/limit connections to and use of external systems.
	DISCUSSION External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented safeguards on those systems. External systems include, for example, personally owned systems or devices and privately-owned computing and communications devices resident in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of CUI, including accessing

	cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational systems. Organizations establish terms and conditions for the use of external systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum, the types of applications that can be accessed on organizational systems from external systems. If terms and conditions with the owners of external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. This requirement recognizes that there are circumstances where individuals using external systems (e.g., contractors, coalition partners) need to access organizational systems. In those situations, organizations need confidence that the external systems contain the necessary safeguards so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required safeguards have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the assurance or confidence level required by organizations. Note that while “external” typically refers to outside of the organization’s direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. And among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered “external" to that system.
3.1.21	**SECURITY REQUIREMENT** Limit use of organizational portable storage devices on external systems.
	DISCUSSION Limits on the use of organization-controlled portable storage devices in external systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used. Note that while “external” typically refers to outside of the organization’s direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. And among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered “external" to that system.
3.1.22	**SECURITY REQUIREMENT** Control CUI posted or processed on publicly accessible systems.
	DISCUSSION In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, CUI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post CUI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.

TABLE E-2: DISCUSSION ON AWARENESS AND TRAINING REQUIREMENTS

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.
	DISCUSSION Organizations determine the content and frequency of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, formal training, offering supplies inscribed with security reminders, generating email advisories or notices from organizational officials, displaying logon screen messages, displaying posters, and conducting information security awareness events. NIST Special Publication 800-50 provides guidance on security awareness and training programs.
3.2.2	**SECURITY REQUIREMENT** Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
	DISCUSSION Organizations determine the content and frequency of security training based on the assigned duties, roles, and responsibilities of individuals and the security requirements of organizations and the systems to which personnel have authorized access. In addition, organizations provide system developers, enterprise architects, security architects, acquisition/procurement officials, software developers, system developers, system or network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards. Such training can include, for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. NIST Special Publication 800-181 provides guidance on role-based information security training in the workplace.
3.2.3	**SECURITY REQUIREMENT** Provide security awareness training on recognizing and reporting potential indicators of insider threat.
	DISCUSSION Potential indicators and possible precursors of insider threat include behaviors such as: inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations).

TABLE E-3: DISCUSSION ON AUDIT AND ACCOUNTABILITY REQUIREMENTS

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.
	DISCUSSION An event is any observable occurrence in a system. Organizations identify event types for which a logging functionality is needed as those events which are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include, for example, password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the monitoring and auditing appropriate for each of the CUI security requirements. Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of event types, the logging necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloud-based architectures. Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred). Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit log information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. Audit logs should be reviewed and analyzed as often as needed to provide important information to organizations to facilitate risk-based decision making. NIST Special Publication 800-92 provides guidance on security log management.
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.
	DISCUSSION This requirement ensures that the contents of the audit record include the information needed to link the audit event to the actions of an individual to the extent feasible. Audit record review, analysis, and reporting covers information security-related logging performed by organizations including, for example, logging that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, use of maintenance tools, nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, system component inventory, communications at the system boundaries, use of mobile code, and use of VoIP.

	Audit records can be generated from many different system components. The list of event types is the set of events for which logs are to be generated. These events are typically a subset of all events for which the system can generate audit records.
3.3.3	**SECURITY REQUIREMENT** Review and update logged events.
	DISCUSSION The intent of this requirement is to periodically re-evaluate which of the logged events will continue to be included in the list of events to be logged. Over time, the event types that are logged by organizations may change. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.
3.3.4	**SECURITY REQUIREMENT** Alert in the event of an audit logging process failure.
	DISCUSSION Audit logging process failures include, for example, software/hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded. This requirement applies to each audit record data storage repository (i.e., distinct system component where audit records are stored), the total audit record storage capacity of organizations (i.e., all audit record data storage repositories combined), or both.
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.
	DISCUSSION Correlating these processes helps to ensure that they do not operate independently but rather collectively. Regarding the assessment of a given organizational system, the requirement is agnostic as to whether this correlation is applied at the system level or at the organization level across all systems.
3.3.6	**SECURITY REQUIREMENT** Provide audit record reduction and report generation to support on-demand analysis and reporting.
	DISCUSSION Audit record reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or organizational entities conducting auditing activities. Audit record reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can help generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the time stamp in the record is insufficient.
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.
	DISCUSSION Time stamps generated by the system include date and time. Time is expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, for example, clocks synchronizing within hundreds of

	milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. This requirement provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network. See IETF Network Time Protocol.
3.3.8	**SECURITY REQUIREMENT** Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
	DISCUSSION Audit information includes all information (e.g., audit records, audit log settings, and audit reports) needed to successfully audit system activity. Audit logging tools are those programs and devices used to conduct audit and logging activities. This requirement focuses on the technical protection of audit information and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by media protection and physical and environmental protection requirements.
3.3.9	**SECURITY REQUIREMENT** Limit management of audit logging functionality to a subset of privileged users.
	DISCUSSION Individuals with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit logging activities or modifying audit records. This requirement specifies that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

TABLE E-4: DISCUSSION ON CONFIGURATION MANAGEMENT REQUIREMENTS

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.
	DISCUSSION This requirement establishes baseline configurations for systems and system components including communications and connectivity aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon sets of specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and changes to systems. Baseline configurations include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture. Baseline configurations of systems reflect the current enterprise architecture. Maintaining effective baseline configurations requires creating new baselines as organizational systems change over time. Baseline configuration maintenance includes reviewing and updating the baseline configuration when changes are made based on security risks and deviations from the established baseline configuration Organizations can implement centralized system component inventories that include components from multiple organizational systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., system association, system owner). Information deemed necessary for effective accountability of system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. NIST Special Publication 800-128 provides guidance on security-focused configuration management
3.4.2	**SECURITY REQUIREMENT** Establish and enforce security configuration settings for information technology products employed in organizational systems.
	DISCUSSION Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers, workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, devices, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security parameters are those parameters impacting the security state of systems including the parameters required to satisfy other security requirements. Security parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the systems configuration baseline. Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other

	organizations in the public and private sectors. NIST Special Publications 800-70 and 800-128 provide guidance on security configuration settings.
3.4.3	**SECURITY REQUIREMENT** Track, review, approve or disapprove, and log changes to organizational systems.
	DISCUSSION Configuration change controls for organizational systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities. Processes for managing configuration changes to systems include, for example, Configuration Control Boards or Change Advisory Boards that review and approve proposed changes to systems. For new development systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards or Change Advisory Boards. Audit logs of changes include activities before and after changes are made to organizational systems and the activities required to implement such changes. NIST Special Publication 800-128 provides guidance on configuration change control.
3.4.4	**SECURITY REQUIREMENT** Analyze the security impact of changes prior to implementation.
	DISCUSSION Organizational personnel with information security responsibilities (e.g., system administrators, system security officers, system security managers, and systems security engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security requirements and reviewing system design documentation to understand the implementation of safeguards and how specific changes might affect the safeguards. Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional safeguards are required. NIST Special Publication 800-128 provides guidance on configuration change control and security impact analysis.
3.4.5	**SECURITY REQUIREMENT** Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
	DISCUSSION Any changes to the hardware, software, or firmware components of systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes, including upgrades and modifications. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access control requirements, workflow automation, media libraries, abstract layers (e.g., changes implemented into external interfaces rather than directly into systems), and change windows (e.g., changes occur only during specified times). In addition to security concerns, commonly-accepted due diligence for configuration management includes access restrictions as an essential part in ensuring the ability to effectively manage the configuration. NIST Special Publication 800-128 provides guidance on configuration change control.

3.4.6	**SECURITY REQUIREMENT** Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.
	DISCUSSION Systems can provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. It is sometimes convenient to provide multiple services from single system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per component. Organizations review functions and services provided by systems or components of systems, to determine which functions and services are candidates for elimination. Organizations disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.
3.4.7	**SECURITY REQUIREMENT** Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
	DISCUSSION Restricting the use of nonessential software (programs) includes, for example, restricting the roles allowed to approve program execution; prohibiting auto-execute; program blacklisting and whitelisting; or restricting the number of program instances executed at the same time.
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.
	DISCUSSION The process used to identify software programs that are not authorized to execute on systems is commonly referred to as blacklisting. The process used to identify software programs that are authorized to execute on systems is commonly referred to as whitelisting. Whitelisting is the stronger of the two policies for restricting software program execution. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup. NIST Special Publication 800-167 provides guidance on application whitelisting.
3.4.9	**SECURITY REQUIREMENT** Control and monitor user-installed software.
	DISCUSSION If provided the necessary privileges, users can install software in organizational systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include, for example, updates and security patches to existing software and downloading applications from organization-approved “app stores.” Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods, automated methods, or both.

TABLE E-5: DISCUSSION ON IDENTIFICATION AND AUTHENTICATION REQUIREMENTS

3.5.1	**SECURITY REQUIREMENT** Identify system users, processes acting on behalf of users, and devices.
	DISCUSSION Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. NIST Special Publication 800-63 provides guidance on digital identities.
3.5.2	**SECURITY REQUIREMENT** Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
	DISCUSSION Individual authenticators include, for example, passwords, key cards, cryptographic devices, and one-time password devices. Initial authenticator content is the actual content of the authenticator, for example, the initial password. In contrast, the requirements about authenticator content include, for example, the minimum password length. Developers ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. NIST Special Publication 800-63 provides guidance on digital identities.
3.5.3	**SECURITY REQUIREMENT** Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
	DISCUSSION Multifactor authentication requires the use of two or more different factors to authenticate. The factors are defined as something you know (e.g., password, personal identification number [PIN]); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). Multifactor solutions that feature physical authenticators include, for example, hardware authenticators providing time-based or challenge-response authenticators and smart cards. In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, when necessary, to provide increased information security. Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of

	information traversing the network. NIST Special Publication 800-63 provides guidance on digital identities.
3.5.4	**SECURITY REQUIREMENT** Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
	DISCUSSION Authentication processes resist replay attacks if it is impractical to successfully authenticate by recording or replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators. NIST Special Publication 800-63 provides guidance on digital identities.
3.5.5	**SECURITY REQUIREMENT** Prevent reuse of identifiers for a defined period.
	DISCUSSION Identifiers are provided for users, processes acting on behalf of users, or devices (3.5.1). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.
3.5.6	**SECURITY REQUIREMENT** Disable identifiers after a defined period of inactivity.
	DISCUSSION Inactive identifiers pose a risk to organizational information because attackers may exploit an inactive identifier to gain undetected access to organizational devices. The owners of the inactive accounts may not notice if unauthorized access to the account has been obtained.
3.5.7	**SECURITY REQUIREMENT** Enforce a minimum password complexity and change of characters when new passwords are created.
	DISCUSSION This requirement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are used as part of multifactor authenticators. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.
3.5.8	**SECURITY REQUIREMENT** Prohibit password reuse for a specified number of generations.
	DISCUSSION Password lifetime restrictions do not apply to temporary passwords.
3.5.9	**SECURITY REQUIREMENT** Allow temporary password use for system logons with an immediate change to a permanent password.
	DISCUSSION Changing temporary passwords to permanent passwords immediately after system logon ensures that the necessary strength of the authentication mechanism is implemented at the earliest opportunity, reducing the susceptibility to authenticator compromises.

3.5.10	**SECURITY REQUIREMENT** Store and transmit only cryptographically-protected passwords.
	DISCUSSION Cryptographically-protected passwords include, for example, salted one-way cryptographic hashes of passwords. See NIST Cryptographic Standards.
3.5.11	**SECURITY REQUIREMENT** Obscure feedback of authentication information.
	DISCUSSION The feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems or system components, for example, desktop or notebook computers with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with small displays, this threat may be less significant, and is balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring authenticator feedback includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

TABLE E-6: DISCUSSION ON INCIDENT RESPONSE REQUIREMENTS

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.
	DISCUSSION Organizations recognize that incident handling capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Organizations consider incident handling as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive. As part of user response activities, incident response training is provided by organizations and is linked directly to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the system; system administrators may require additional training on how to handle or remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification/reporting of suspicious activities from external and internal sources. User response activities also includes incident response assistance which may consist of help desk support, assistance groups, and access to forensics services or consumer redress services, when required. NIST Special Publication 800-61 provides guidance on incident handling. NIST Special Publications 800-86 and 800-101 provide guidance on integrating forensic techniques into incident response.
3.6.2	**SECURITY REQUIREMENT** Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
	DISCUSSION Tracking and documenting system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Reporting incidents addresses specific incident reporting requirements within an organization and the formal incident reporting requirements for the organization. Suspected security incidents may also be reported and include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, and policies. NIST Special Publication 800-61 provides guidance on incident handling.
3.6.3	**SECURITY REQUIREMENT** Test the organizational incident response capability.
	DISCUSSION Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel and full

	interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. NIST Special Publication 800-84 provides guidance on testing programs for information technology capabilities.

TABLE E-7: DISCUSSION ON MAINTENANCE REQUIREMENTS

3.7.1	**SECURITY REQUIREMENT** Perform maintenance on organizational systems.
	DISCUSSION This requirement addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity. System maintenance also includes those components not directly associated with information processing and data or information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: date and time of maintenance; name of individuals or group performing the maintenance; name of escort, if necessary; a description of the maintenance performed; and system components or equipment removed or replaced (including identification numbers, if applicable).
3.7.2	**SECURITY REQUIREMENT** Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
	DISCUSSION This requirement addresses security-related issues with maintenance tools that are not within the organizational system boundaries that process, store, or transmit CUI, but are used specifically for diagnostic and repair actions on those systems. Organizations have flexibility in determining the controls in place for maintenance tools, but can include approving, controlling, and monitoring the use of such tools. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational systems. Maintenance tools can include, for example, hardware and software diagnostic test equipment and hardware and software packet sniffers.
3.7.3	**SECURITY REQUIREMENT** Ensure equipment removed for off-site maintenance is sanitized of any CUI.
	DISCUSSION See discussion for 3.7.1. NIST Special Publication 800-88 provides guidance on media sanitization.
3.7.4	**SECURITY REQUIREMENT** Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
	DISCUSSION See discussion for 3.7.2.
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.
	DISCUSSION Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through an external network. Authentication techniques used in the establishment of these nonlocal maintenance and diagnostic sessions reflect the network access requirements in 3.5.3.

3.7.6	**SECURITY REQUIREMENT** Supervise the maintenance activities of maintenance personnel without required access authorization.
	DISCUSSION This requirement applies to individuals performing hardware or software maintenance on organizational systems, while 3.10.1 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, consultants, and systems integrators, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Organizations may choose to issue temporary credentials to these individuals based on organizational risk assessments. Temporary credentials may be for one-time use or for very limited time periods.

TABLE E-8: DISCUSSION ON MEDIA PROTECTION REQUIREMENTS

3.8.1	**SECURITY REQUIREMENT** Protect (i.e. physically control and securely store) system media containing CUI, both paper and digital.
	DISCUSSION System media includes digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Protecting digital media includes, for example, limiting access to design specifications stored on compact disks or flash drives in the media library to the project leader and any individuals on the development team. Physically controlling system media includes, for example, conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. Access to CUI on system media can be limited by physically controlling such media, which includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. NIST Special Publication 800-111 provides guidance on storage encryption technologies for end user devices.
3.8.2	**SECURITY REQUIREMENT** Limit access to CUI on system media to authorized users.
	DISCUSSION System media includes digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external or removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library.
3.8.3	**SECURITY REQUIREMENT** Sanitize or destroy system media containing CUI before disposal or release for reuse.
	DISCUSSION This requirement applies to all system media, digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include: digital media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, destruction, removing CUI from a document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control the sanitization process for controlled unclassified information. See NARA

	Sanitization Policy and Guidance. NIST Special Publication 800-88 provides guidance on media sanitization.
3.8.4	**SECURITY REQUIREMENT** Mark media with necessary CUI markings and distribution limitations.
	DISCUSSION The term *security marking* refers to the application or use of human-readable security attributes. System media includes digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external or removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Marking of system media reflects applicable federal laws, Executive Orders, directives, policies, and regulations. See NARA Marking Handbook.
3.8.5	**SECURITY REQUIREMENT** Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
	DISCUSSION System media includes digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external or removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Controlled areas are areas or spaces for which organizations provide sufficient physical or procedural safeguards to meet the requirements established for protecting systems and information. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization. Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of system media in accordance with organizational risk assessments to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records.
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.
	DISCUSSION This requirement applies to portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, and e-readers). NIST Special Publication 800-111 provides guidance on storage encryption technologies for end user devices. See NIST Cryptographic Standards.
3.8.7	**SECURITY REQUIREMENT** Control the use of removable media on system components.

	DISCUSSION System media includes digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external or removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This requirement also applies to mobile devices with information storage capability (e.g., smart phones, tablets, and e-readers). In contrast to 3.8.1, which restricts user access to media, this requirement restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to control the use of system media. Organizations may control the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may control the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices.
3.8.8	**SECURITY REQUIREMENT** Prohibit the use of portable storage devices when such devices have no identifiable owner.
	DISCUSSION Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code).
3.8.9	**SECURITY REQUIREMENT** Protect the confidentiality of backup CUI at storage locations.
	DISCUSSION Backed-up information containing CUI may include system-level information and user-level information. System-level information includes, for example, system-state information, operating system software and application software, and licenses. User-level information includes information other than system-level information. Organizations can employ cryptographic mechanisms or alternative physical safeguards to protect the confidentiality of backup information at designated storage locations.

TABLE E-9: DISCUSSION ON PERSONNEL SECURITY REQUIREMENTS

3.9.1	**SECURITY REQUIREMENT** Screen individuals prior to authorizing access to organizational systems containing CUI.
	DISCUSSION Personnel screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.
3.9.2	**SECURITY REQUIREMENT** Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.
	DISCUSSION Protecting CUI during and after personnel actions may include, for example, return of system-related property and exit interviews. System-related property includes, for example, hardware authentication tokens, identification cards, system administration technical manuals, keys, and building passes. Exit interviews ensure that individuals who have been terminated understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. For termination actions, timely execution is essential for individuals terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified. This requirement applies to reassignments or transfers of individuals when the personnel action is permanent or of such extended durations as to require protection. Organizations define the CUI protections appropriate for the types of reassignments or transfers, whether permanent or extended. Protections that may be required for transfers or reassignments to other positions within organizations include, for example: returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

TABLE E-10: DISCUSSION ON PHYSICAL PROTECTION REQUIREMENTS

3.10.1	**SECURITY REQUIREMENT** Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
	DISCUSSION This requirement applies to organizational employees, individuals with permanent physical access authorization credentials, and visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible. Limiting physical access to equipment may include, for example, placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only, and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external hard disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.
3.10.2	**SECURITY REQUIREMENT** Protect and monitor the physical facility and support infrastructure for organizational systems.
	DISCUSSION Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished, for example, by the employment of guards; the use of sensor devices; or the use of video surveillance equipment such as cameras. Examples of support infrastructure include system distribution, transmission, and power lines. Security safeguards applied to the support infrastructure prevent accidental damage, disruption, and physical tampering. Such safeguards may also be necessary to help prevent eavesdropping or modification of unencrypted transmissions. Safeguards used to control physical access to support infrastructure include, for example, locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.
3.10.3	**SECURITY REQUIREMENT** Escort visitors and monitor visitor activity.
	DISCUSSION This requirement applies to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional security staff or administrative staff or system users. Physical access control systems comply with applicable laws, Executive Orders, directives, policies, regulations, and standards. Audit logs can be used to monitor visitor activity.
3.10.4	**SECURITY REQUIREMENT** Maintain audit logs of physical access.
	DISCUSSION Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both. Components of systems (e.g., workstations, notebook computers, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices.

3.10.5	**SECURITY REQUIREMENT** Control and manage physical access devices.
	DISCUSSION Physical access devices include, for example, keys, locks, combinations, and card readers.
3.10.6	**SECURITY REQUIREMENT** Enforce safeguarding measures for CUI at alternate work sites.
	DISCUSSION Alternate work sites may include, for example, government facilities or private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. NIST Special Publications 800-46 and 800-114 provide guidance on enterprise and user security when teleworking.

TABLE E-11: DISCUSSION ON RISK ASSESSMENT REQUIREMENTS

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.
	DISCUSSION Clearly defined system boundaries are a prerequisite for effective risk assessments. Such risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of organizational systems. Risk assessments also consider risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities). Risk assessments, either formal or informal, can be conducted at the organization level, the mission or business process level, or the system level, and at any phase in the system development life cycle. NIST Special Publication 800-30 provides guidance on conducting risk assessments.
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.
	DISCUSSION Organizations determine the required vulnerability scanning for all system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This process ensures that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in source code reviews and in a variety of tools (e.g., static analysis tools, web-based application scanners, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms. Scanning tools that facilitate interoperability include, for example, products that are Security Content Automated Protocol (SCAP)-validated. Thus, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Security assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates thorough vulnerability scanning and protects the sensitive nature of such scanning. NIST Special Publication 800-40 provides guidance on vulnerability management.
3.11.3	**SECURITY REQUIREMENT** Remediate vulnerabilities in accordance with risk assessments.
	DISCUSSION Vulnerabilities discovered, for example, via the scanning conducted in response to 3.11.2, are remediated with consideration of the related assessment of risk. The consideration of risk

	influences the prioritization of remediation efforts and the level of effort to be expended in the remediation for specific vulnerabilities.

TABLE E-12: DISCUSSION ON SECURITY ASSESSMENT REQUIREMENTS

3.12.1	**SECURITY REQUIREMENT** Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
	DISCUSSION Organizations assess security controls in organizational systems and the environments in which those systems operate as part of system development life cycle activities. Security assessments ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls as documented in system security plans. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Organizations can choose to use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of systems during the life cycle. NIST Special Publication 800-53A provides guidance on developing security assessment plans and for conducting assessments. NIST Special Publication 800-53 provides guidance on security and privacy controls for systems and organizations.
3.12.2	**SECURITY REQUIREMENT** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
	DISCUSSION The plan of action is a key document in the information security program. Organizations develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format. Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.
3.12.3	**SECURITY REQUIREMENT** Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
	DISCUSSION Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms *continuous* and *ongoing* imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Providing access to security information on a continuing basis through reports or dashboards gives organizational officials the capability to make more effective and timely risk management decisions. Automation supports more frequent updates to hardware, software, firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely.

	Monitoring requirements, including the need for specific monitoring, may also be referenced in other requirements. NIST Special Publication 800-137 provides guidance on continuous monitoring.
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.
	DISCUSSION Security plans relate security requirements to a set of security controls. Security plans also describe, at a high level, how the security controls meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls. Security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk if the plan is implemented as intended. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization. NIST Special Publication 800-18 provides guidance on developing security plans.

TABLE E-13: DISCUSSION ON SYSTEM AND COMMUNICATIONS PROTECTION REQUIREMENTS

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.
	DISCUSSION Boundary components include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Restricting or prohibiting interfaces in organizational systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. NIST Special Publication 800-41 provides guidance on firewalls and firewall policy. NIST Special Publication 800-125 provides guidance on security for virtualization technologies.
3.13.2	**SECURITY REQUIREMENT** Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
	DISCUSSION Organizations apply systems security engineering principles to new development systems or systems undergoing major upgrades. For legacy systems, organizations apply systems security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security engineering concepts and principles helps to develop trustworthy, secure, and resilient systems and system components and reduce the susceptibility of organizations to disruptions, hazards, and threats. Examples of these concepts and principles include developing layered protections; establishing security policies, architecture, and controls as the foundation for design; incorporating security requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk-management decisions. NIST Special Publication 800-160 provides guidance on systems security engineering.
3.13.3	**SECURITY REQUIREMENT** Separate user functionality from system management functionality.
	DISCUSSION System management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from system management functionality is physical or logical. Organizations can implement separation of system management functionality from user functionality by using different computers, different central processing units, different instances of operating systems, or different network addresses; virtualization techniques; or combinations of

	these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.
3.13.4	**SECURITY REQUIREMENT** Prevent unauthorized and unintended information transfer via shared system resources.
	DISCUSSION This requirement prevents information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to any current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources (e.g., registers, cache memory, main memory, hard disks) after those resources have been released back to the system. This requirement also applies to encrypted representations of information. The control of information in shared system resources is also commonly referred to as object reuse and residual information protection. This requirement does not address information remanence, which refers to residual representation of data that has been nominally deleted; covert channels (including storage or timing channels) where shared resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.
3.13.5	**SECURITY REQUIREMENT** Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
	DISCUSSION Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. DMZs are typically implemented with boundary control devices and techniques that include, for example, routers, gateways, routers, firewalls, virtualization, and/or cloud-based technologies. NIST Special Publication 800-41 provides guidance on firewalls and firewall policy. NIST Special Publication 800-125 provides guidance on security for virtualization technologies.
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).
	DISCUSSION This requirement applies to inbound and outbound network communications traffic, both at the system boundary and at identified points within the system. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.
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).
	DISCUSSION This requirement is implemented in remote devices (e.g., notebook computers, tablets) through configuration settings to disable split tunneling in those devices, and by preventing configuration settings from being readily configurable by users. This requirement is implemented in the system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local system resources such as

	printers or file servers. However, split tunneling would allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information.
3.13.8	**SECURITY REQUIREMENT** Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
	DISCUSSION This requirement applies to internal and external networks and any system components that can transmit information including, for example, servers, mobile devices, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, and facsimile machines. Communication paths outside the physical protection of a controlled boundary are susceptible to interception and modification. Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed safeguards for transmission confidentiality. In such situations, organizations determine what types of confidentiality services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary safeguards and assurances of the effectiveness of the safeguards through appropriate contracting vehicles, organizations implement compensating safeguards or explicitly accept the additional risk. An example of an alternative physical safeguard is a protected distribution system (PDS) where the distribution medium is protected against electronic or physical intercept, thereby ensuring the confidentiality of the information being transmitted. See NIST Cryptographic Standards.
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.
	DISCUSSION This requirement applies to internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address or port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of user inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses.
3.13.10	**SECURITY REQUIREMENT** Establish and manage cryptographic keys for cryptography employed in organizational systems.
	DISCUSSION Cryptographic key management and establishment can be performed using manual procedures or mechanisms supported by manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, and standards, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key maintenance.
3.13.11	**SECURITY REQUIREMENT** Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

	DISCUSSION Cryptography can be employed to support many security solutions including, for example, the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on other security requirements, organizations define each type of cryptographic use and the type of cryptography required (e.g., FIPS-validated cryptography). See NIST Cryptographic Standards; NIST Cryptographic Module Validation Program; NIST Cryptographic Algorithm Validation Program.
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.
	DISCUSSION Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Indication of use includes, for example, signals to users when collaborative computing devices are activated. Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.
3.13.13	**SECURITY REQUIREMENT** Control and monitor the use of mobile code.
	DISCUSSION Decisions regarding the use of mobile code in organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations, notebook computers, and devices (e.g., smart phones). Mobile code policy and procedures address controlling or preventing the development, acquisition, or introduction of unacceptable mobile code in systems, including, for example, requiring mobile code to be digitally signed by a trusted source. NIST Special Publication 800-28 provides guidance on mobile code.
3.13.14	**SECURITY REQUIREMENT** Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
	DISCUSSION VoIP has different requirements, features, functionality, availability, and service limitations when compared with Plain Old Telephone Service (POTS) (i.e., the standard telephone service that most homes use). In contrast, other telephone services are based on high-speed, digital communications lines, such as ISDN and FDDI. The main distinctions between POTS and non-POTS services are speed and bandwidth. To address the threats associated with VoIP, usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if it is used maliciously. Threats to VoIP are similar to those inherent with any Internet-based application. NIST Special Publication 800-58 provides guidance on Voice Over IP Systems.
3.13.15	**SECURITY REQUIREMENT** Protect the authenticity of communications sessions.
	DISCUSSION

	This requirement addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into sessions. NIST Special Publications 800-52, 800-77, 800-95, and 800-113 provide guidance on secure communications sessions.
3.13.16	**SECURITY REQUIREMENT** Protect the confidentiality of CUI at rest.
	DISCUSSION This requirement addresses the confidentiality of information at rest. Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The focus of protection at rest is not on the type of storage device or the frequency of access but rather the state of the information. Organizations can use different mechanisms to achieve confidentiality protections, including the use of cryptographic mechanisms and file share scanning. Organizations may also employ other safeguards including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved or continuous monitoring to identify malicious code at rest. See NIST Cryptographic Standards.

TABLE E-14: DISCUSSION ON SYSTEM AND INFORMATION INTEGRITY REQUIREMENTS

3.14.1	**SECURITY REQUIREMENT** Identify, report, and correct system flaws in a timely manner.
	DISCUSSION Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws, and report this information to designated personnel with information security responsibilities. Security-relevant updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational systems. By incorporating flaw remediation into configuration management processes, any required or anticipated remediation actions can be tracked and verified. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types or remediation. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. NIST Special Publication 800-40 provides guidance on patch management technologies.
3.14.2	**SECURITY REQUIREMENT** Provide protection from malicious code at designated locations within organizational systems.
	DISCUSSION Appropriate locations include system entry and exit points which may include, for example, firewalls, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, or actions

	in response to detection of maliciousness when attempting to open or execute files. NIST Special Publication 800-83 provides guidance on malware incident prevention.
3.14.3	**SECURITY REQUIREMENT** Monitor system security alerts and advisories and take action in response.
	DISCUSSION The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government and in nonfederal organizations. Software vendors, subscription services, and relevant industry information sharing and analysis centers (ISACs) may also provide security alerts and advisories. Security directives are issued by designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be followed and corrective actions implemented in a timely manner. Examples of response actions include notifying relevant external organizations, for example, external mission/business partners, supply chain partners, external service providers, and other peer or supporting organizations.
3.14.4	**SECURITY REQUIREMENT** Update malicious code protection mechanisms when new releases are available.
	DISCUSSION Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.
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.
	DISCUSSION See discussion for 3.14.2.
3.14.6	**SECURITY REQUIREMENT** Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
	DISCUSSION System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system. Organizations can monitor systems, for example, by observing audit record activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. System monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software).

	Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices being employed at managed system interfaces. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of systems to support such objectives. System monitoring is an integral part of continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Unusual or unauthorized activities or conditions related to inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements. NIST Special Publication 800-94 provides guidance on intrusion detection and prevention systems.
3.14.7	**SECURITY REQUIREMENT** Identify unauthorized use of organizational systems.
	DISCUSSION See discussion for 3.14.6.