Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date March 15, 2022

Original Release Date April 27, 2021

Superseding Document

Status	Final
Series/Number	NIST Special Publication 800-172A
Title	Assessing Enhanced Security Requirements for Controlled Unclassified Information
Publication Date	March 2022
DOI	https://doi.org/10.6028/NIST.SP.800-172A
CSRC URL	https://csrc.nist.gov/publications/detail/sp/800-172a/final
Additional Information	https://csrc.nist.gov/projects/protecting-controlled-unclassified-information

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

Draft NIST Special Publication 800-172A

Assessing Enhanced Security Requirements for Controlled Unclassified Information

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-172A-draft

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

Draft NIST Special Publication 800-172A

Assessing Enhanced Security Requirements for Controlled Unclassified Information

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-172A-draft

April 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA), 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 the 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, OMB Director, 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 800-172A
Natl. Inst. Stand. Technol. Spec. Publ. 800-172A, **62 pages** (April 2021)

CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-172A-draft

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 public comment periods and provide feedback to NIST. Many NIST publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: April 27, 2021 through June 11, 2021

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) [FOIA96].

Reports on Computer Systems Technology

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

Abstract

The protection of Controlled Unclassified Information (CUI) in nonfederal systems and organizations is important to federal agencies and can directly impact the ability of the Federal Government to successfully carry out its assigned missions and business operations. This publication provides federal agencies and nonfederal organizations with assessment procedures that can be used to carry out assessments of the requirements in NIST Special Publication 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*. The assessment procedures are flexible and can be tailored to the needs of organizations and assessors. Assessments can be conducted as 1) self-assessments; 2) independent, third-party assessments; or 3) government-sponsored assessments. The assessments can be conducted with varying degrees of rigor based on customer-defined depth and coverage attributes. The findings and evidence produced during the assessments can be used to facilitate risk-based decisions by organizations related to the CUI enhanced security requirements.

Keywords

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

70 # Acknowledgements

71 The authors wish to recognize the research staff from the NIST Computer Security Division and
72 the Applied Cybersecurity Division for their contributions in helping to improve the content of
73 this publication. A special note of thanks to Pat O'Reilly, Jim Foti, Jeff Brewer, Ned Goren, Chris
74 Enloe, and the entire NIST web team for their outstanding administrative support. The authors
75 also wish to acknowledge the contributions from individuals and organizations in the public and
76 private sectors, nationally and internationally, whose thoughtful and constructive comments
77 improved the overall quality, thoroughness, and usefulness of this publication.

Notes to Reviewers

This publication is intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the enhanced security requirements in NIST Special Publication 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*. This objective is accomplished by:

- Providing flexible and tailorable assessment procedures for the CUI enhanced security requirements;
- Defining assessment objectives to help guide and inform the assessment;
- Specifying potential assessment methods that can be used to generate evidence and produce findings and results;
- Describing a set of potential 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 supplemental guidance to explain and interpret the CUI enhanced security requirements.

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 security assessment plans and approaches that can produce the evidence needed for risk-based decisions or to determine compliance to the CUI enhanced 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 approach taken to incorporating organization-defined parameters into determination statements for the assessment objectives.

As always, your feedback is very important to us. We appreciate each and every contribution from our reviewers. The insightful comments from the public and private sectors continue to help shape the final publication to ensure that it meets the needs and expectations of our customers.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i) under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii) without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: sec-cert@nist.gov.

135

CAUTIONARY NOTE

The generalized assessment procedures described in this publication provide a framework and starting point for developing specific procedures to assess the enhanced security requirements in NIST Special Publication 800-172. The assessment procedures can be used to help generate and evaluate the relevant evidence needed to determine if the security safeguards employed by organizations are implemented correctly, operating as intended, and satisfy the enhanced security requirements. Organizations have the flexibility to tailor the assessment procedures by selecting the specific assessment methods and objects to achieve the assessment objectives. There is no expectation that all assessment methods and objects will be used for every assessment. There is also significant flexibility in the scope of the assessment and the degree of rigor applied during the assessment process. The assessment procedures can be employed in self-assessments, independent, third-party assessments, or assessments conducted by sponsoring organizations (e.g., government agencies). Such approaches may be specified in contracts or in agreements by participating parties.

136

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.

Table of Contents

Errata

This table contains changes that have been incorporated into Special Publication 800-172A. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature. Any potential updates for this document that are not yet published in an errata update or revision—including additional issues and potential corrections—will be posted as they are identified. See SP 800-172A publication details.

DATE	TYPE	CHANGE	PAGE

CHAPTER ONE

INTRODUCTION

THE NEED TO ASSESS ENHANCED SECURITY REQUIREMENTS FOR CUI

In 2010, Executive Order 13556 established a government-wide Controlled Unclassified Information (CUI) Program to standardize the way that the executive branch handles unclassified information that requires protection. The regulation that implements the CUI Program is 32 CFR part 2002. Only federal information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or government-wide policy may be designated as CUI.[1] NIST Special Publication (SP) 800-172, a supplement to NIST SP 800-171, specifies enhanced security requirements to ensure the confidentiality, integrity, and availability of CUI when it is associated with a high-value asset or a critical program.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to describe procedures for assessing the enhanced security requirements in [SP 800-172]. Compliance with the security requirements is addressed in CUI guidance and the CUI Federal Acquisition Regulation (FAR) 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 enhanced security requirements have been satisfied. The assessment procedures are typically used as part of an assessment process. An assessment process is an information-gathering and evidence-producing activity to determine the effectiveness of the safeguards implemented to meet the set of security requirements specified in [SP 800-172]. The information gathered and evidence produced can be used by an organization to:

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

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

[1] The National Archives and Records Administration CUI Registry [NARA CUI] is the online repository for information, guidance, policy, and requirements on handling CUI.

THE SCOPE OF ENHANCED SECURITY REQUIREMENT ASSESSMENTS

The scope of the assessments conducted using the procedures described in this publication are guided and informed by the system security plans for the organizational systems processing, storing, or transmitting CUI. The assessments focus on the overall effectiveness of the security safeguards intended to satisfy the enhanced security requirements defined in [SP 800-172].

1.2 TARGET AUDIENCE

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

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

1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

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

Chapter Three provides a catalog of assessment procedures for the CUI enhanced security requirements in [SP 800-172], including assessment objectives and potential assessment methods and objects for each procedure.

Supporting appendices provide additional assessment-related information, including general **References**, a **Glossary**, a list of **Acronyms**, and a description of the **Assessment Methods** used in assessment procedures.

CHAPTER TWO

THE FUNDAMENTALS

BASIC CONCEPTS FOR ASSESSMENTS OF CUI ENHANCED SECURITY REQUIREMENTS

The CUI enhanced security requirements in [SP 800-172] are organized into 10 families. Each family contains the requirements related to the general security topic of the family. Table 1 lists the enhanced security requirement families addressed in this publication.[2] The assessment procedures in Chapter Three are grouped by family designations to help ensure completeness and consistency of assessments.

TABLE 1: CUI ENHANCED 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 *objects* that can be used to conduct the assessment. Each assessment objective includes a set of *determination statements* related to the CUI enhanced security requirement that is the subject of the assessment. Organization-defined parameters (ODP) that are part of selected enhanced security requirements are included in the initial determination statements for the assessment procedure. ODPs are included since the specified parameter values are used in subsequent determination statements. ODPs are numbered sequentially and noted in ***bold italics***.

Determination statements reflect the content of the enhanced security requirements to ensure traceability of the assessment results to the requirements. The application of an assessment procedure to an enhanced security requirement produces assessment *findings*. The findings are used to determine if the enhanced security requirement has been satisfied. Assessment objects are associated with the specific items being assessed. These objects can include specifications, mechanisms, activities, and individuals. Specifications are the document-based artifacts (e.g., security policies, procedures, plans, 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

[2] There are 4 families in [SP 800-171] that do not contain enhanced security requirements: Audit and Accountability, Maintenance, Media Protection, and Physical Protection.

system that involve people (e.g., conducting system backup operations, exercising a contingency plan, and monitoring network traffic). Individuals are people applying the specifications, mechanisms, or activities described above.

Assessment methods define the nature and extent of the assessor's actions. The methods include *examine*, *interview*, and *test*. The examine method is the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., mechanisms, activities, specifications). The interview method is the process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence. The test method is the process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior. The purpose of the assessment methods is to facilitate understanding, achieve clarification, and obtain evidence. The results obtained from applying the methods 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 affect the level of effort for the assessment. These attributes provide a means to define the rigor and scope of the assessment to obtain the assurance needed for enhanced security requirements. A description of assessment methods and objects is provided in Appendix C.[3] Figure 1 illustrates an example of an assessment procedure for the CUI enhanced security requirement 3.1.3e from [SP 800-172].

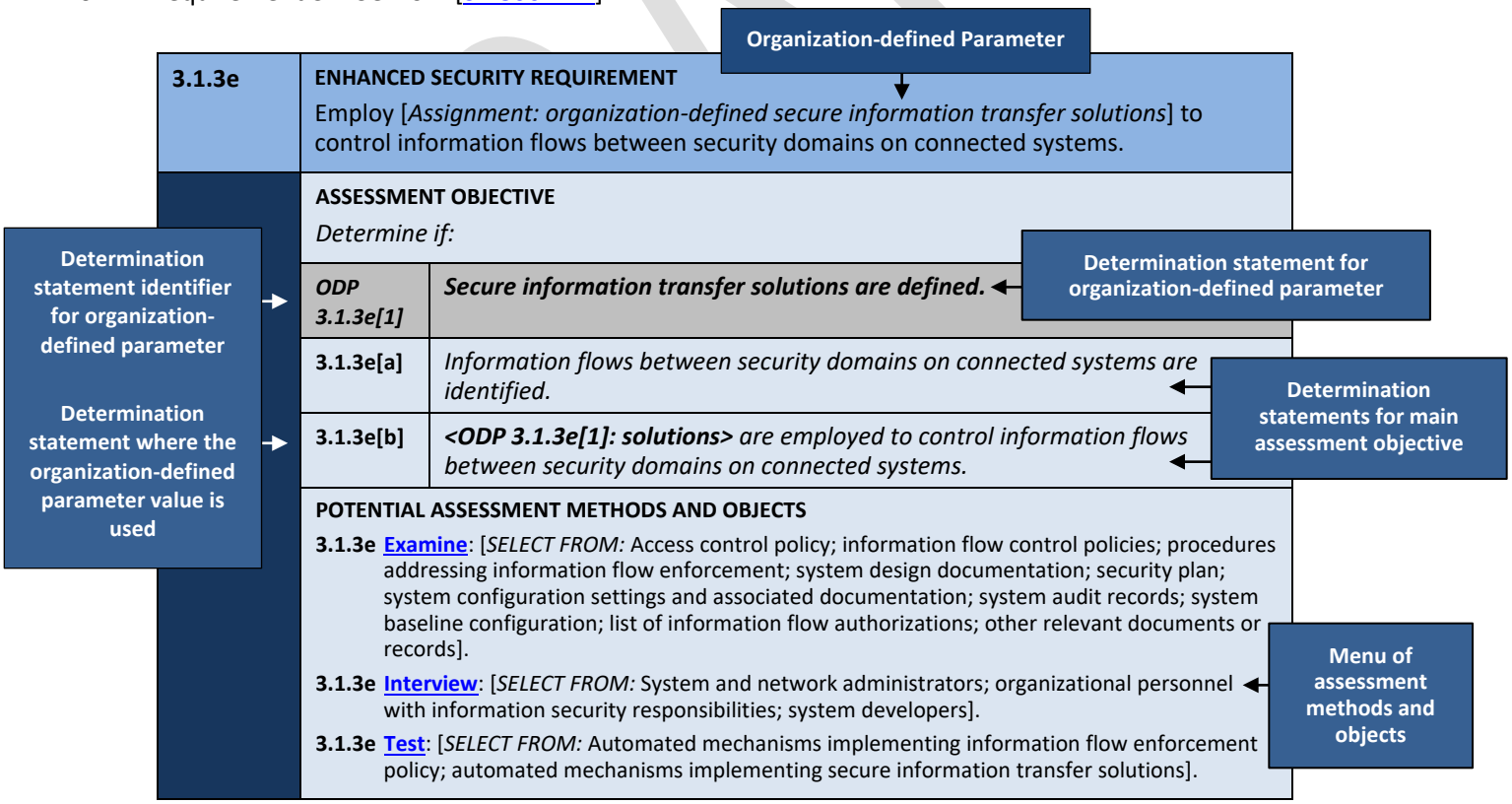

FIGURE 1: ASSESSMENT PROCEDURE FOR CUI ENHANCED SECURITY REQUIREMENT

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

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

ORGANIZATION-DEFINED PARAMETERS

Selected enhanced security requirements contain *selection* and *assignment* operations to give organizations flexibility in defining variable parts of those requirements. Selection operations require organizations to select from a list of predefined items. Assignment operations require organizations to define specific parameter values. Determination statements for organization-defined parameters (ODP) are listed first in the assessment objective section followed by the list of determination statements for the assessment objective. Determination statements for ODPs are noted in ***bold italics***. The ODP values are used in the appropriate determination statements in the assessment procedure, also noted in ***bold italics***.

2.2 ASSURANCE CASES

Building an effective assurance case for determining compliance to the enhanced security requirements is a process that involves compiling evidence from a variety of sources and conducting different types of assessment activities. An assurance case is a body of evidence organized into an argument demonstrating that some claim about a system is true. For the assessments conducted using the procedures in this publication, that claim is compliance with the enhanced security requirements specified in [SP 800-172]. Assessors obtain evidence during the assessment process to allow designated officials[4] to make objective determinations about compliance to the CUI enhanced security requirements. The evidence needed to make such determinations can be obtained from various sources, including self-assessments, independent third-party assessments, government-sponsored assessments, or other types of assessments, depending on the needs of the organization establishing the requirements and the organization conducting the assessments.

For example, some enhanced security requirements are satisfied by security capabilities built into commercial information technology products and systems. Product assessments are typically conducted by independent, third-party testing organizations.[5] These assessments

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

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

examine the security functions of the products and the 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 assessments can be carried out at a greater level of depth and provide deeper insights into the security capabilities of the products.

Ultimately, the evidence needed to determine compliance comes from the implementation of the safeguards to satisfy the enhanced security requirements and from the assessments of that implementation. Assessors can build on previously developed artifacts 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 artifacts, obtained while implementing security throughout the system development life cycle, provide the initial evidence for an assurance case.

Assessments can be conducted by systems developers, systems integrators, system owners, evaluators, auditors, or the security staffs of organizations. The assessors or assessment teams begin by obtaining and reviewing the results from individual component product or compliance assessments. The assessors then determine the additional system-level assessments required to achieve the needed assurance using the procedures and methods contained in this publication and based on the specific implementation information provided by nonfederal organizations in their system security plans. Assessments can be used to compile and evaluate the evidence needed by organizations to determine the effectiveness of the safeguards implemented to protect CUI, the actions needed to mitigate security-related risks, and compliance to the enhanced security requirements.

SECURITY ASSESSMENT PLANS

The system security plan is used to describe how the organization meets or plans to meet the CUI enhanced security requirements. Once the organization completes the system security plan, a security assessment plan can be developed using the appropriate assessment procedures described in Chapter Three. An assessment procedure is developed for every enhanced security requirement that is applicable to the system, system component, or the organization. The assessment procedures are tailored to meet the needs of the organization.

CHAPTER THREE

THE PROCEDURES

ASSESSMENT PROCEDURES, METHODS, AND OBJECTS FOR ENHANCED SECURITY REQUIREMENTS

This chapter provides assessment procedures for the CUI enhanced security requirements defined in [SP 800-172]. The assessment procedures are organized into 10 families, as illustrated in Table 1. Organizations conducting CUI enhanced 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 security assurance 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 C provides additional information on the levels of rigor and detail for assessments.

The assessment objective for an assessment procedure is achieved by applying the designated assessment methods to the selected assessment objects and producing the evidence necessary to make the *determination* associated with the objective. Each determination statement in an assessment procedure produces a finding of either *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) demonstrates 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 demonstrate potential anomalies that may need to be addressed by the organization. The findings may also indicate that for reasons described in the assessment report, the assessor was unable to obtain sufficient information to make the determination.

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

CAUTIONARY NOTE

The content in this publication can be used for many different assessment-related purposes in determining if organizations satisfy the CUI enhanced security requirements in [SP 800-172]. The list of potential assessment methods and objects do not necessarily reflect, and should not be directly associated with, compliance or noncompliance with the requirements. The selection of assessment methods and objects by the organization can help generate the evidence necessary to determine compliance with the enhanced security requirements. There is no expectation about the number of methods or objects needed to determine compliance with the requirements. Moreover, the list of potential assessment objects should not be viewed as required artifacts needed to determine compliance with the requirements. Organizations have the flexibility to determine the specific methods and objects needed to obtain the evidence to support claims of compliance.

3.1 ACCESS CONTROL

3.1.1e	**ENHANCED SECURITY REQUIREMENT** Employ dual authorization to execute critical or sensitive system and organizational operations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.1e[a]	*Critical or sensitive system and organizational operations are identified.*
	3.1.1e[b]	*Dual authorization is employed to execute critical or sensitive system and organizational operations.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **3.1.1e Examine**: [*SELECT FROM:* List of critical or sensitive system and organizational operations; access control policy; dual authorization policy; procedures addressing access enforcement and dual authorization; security plan; configuration management plan; system design documentation; system configuration settings and associated documentation; list of privilege access authorizations; commands requiring dual authorization; list of actions requiring dual authorization; system audit records; list of approved authorizations (user privileges); system generated list of dual authorization credentials or rules; logs or records of deletion or destruction of backup information; list of system media requiring dual authorization for sanitization; authorization records; media sanitization records; audit records; other relevant documents or records]. **3.1.1e Interview**: [*SELECT FROM:* System and network administrators; system developers; organizational personnel with responsibilities for access enforcement, system backup, dual authorization enforcement for implementing system changes, system media sanitization, audit and accountability, information security]. **3.1.1e Test**: [*SELECT FROM:* Automated mechanisms implementing enforcement of dual authorization].	

3.1.2e	**ENHANCED SECURITY REQUIREMENT** Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.2e[a]	*Information resources that are owned, provisioned, or issued by the organization are identified.*
	3.1.2e[b]	*Access to systems and system components is restricted to only those information resources that are owned, provisioned, or issued by the organization.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **3.1.2e Examine**: [*SELECT FROM:* Access control policy; procedures addressing the use of external systems; list of information resources owned, provisioned, or issued by the organization; security plan; system design documentation; system configuration settings and associated documentation; system connection or processing agreements; system audit records; account management documents; other relevant documents or records]. **3.1.2e Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for restricting or prohibiting use of non-organizationally owned systems, system components, or devices; system and network administrators; organizational personnel with system security responsibilities].	

	3.1.2e **Test**: [*SELECT FROM:* Automated mechanisms implementing restrictions on the use of non-organizationally owned systems, components, or devices].

3.1.3e	**ENHANCED SECURITY REQUIREMENT** Employ [*Assignment: organization-defined secure information transfer solutions*] to control information flows between security domains on connected systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.1.3e[1]	***Secure information transfer solutions are defined.***
	3.1.3e[a]	*Information flows between security domains on connected systems are identified.*
	3.1.3e[b]	***<ODP 3.1.3e[1]: solutions>*** *are employed to control information flows between security domains on connected systems.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **3.1.3e** **Examine**: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; security plan; system configuration settings and associated documentation; system audit records; system baseline configuration; list of information flow authorizations; other relevant documents or records]. **3.1.3e** **Interview**: [*SELECT FROM:* System and network administrators; organizational personnel with information security responsibilities; system developers]. **3.1.3e** **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy; automated mechanisms implementing secure information transfer solutions].	

3.2 AWARENESS AND TRAINING

3.2.1e	**ENHANCED SECURITY REQUIREMENT** Provide awareness training [*Assignment: organization-defined frequency*] focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training [*Assignment: organization-defined frequency*] or when there are significant changes to the threat.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.2.1e[1]	***The frequency of providing awareness training is defined.***
	ODP 3.2.1e[2]	***The frequency of updating awareness training is defined.***
	3.2.1e[a]	*Threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors are identified.*
	3.2.1e[b]	*Awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors is provided* ***<ODP 3.2.1e[1]: frequency>****.*

	3.2.1e[c]	*Significant changes to the threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors are identified.*
	3.2.1e[d]	*Awareness training is updated **<ODP 3.2.1e[2]: frequency>** or when there are significant changes to the threat.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Awareness training policy; procedures addressing awareness training implementation; appropriate codes of federal regulations; awareness training curriculum; awareness training materials; security plan; training records; threat information on social engineering, advanced persistent threat actors, suspicious behaviors, and breaches; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for awareness training; organizational personnel with information security responsibilities; organizational personnel comprising the general system user community]. **Test**: [*SELECT FROM:* Automated mechanisms managing awareness training; automated mechanisms managing threat information].	

400
401

3.2.2e	**ENHANCED SECURITY REQUIREMENT** Include practical exercises in awareness training for [*Assignment: organization-defined roles*] that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.2.2e[1]	***Roles to be included in awareness training practical exercises are defined.***
	3.2.2e[a]	*Practical exercises are identified.*
	3.2.2e[b]	*Current threat scenarios are identified.*
	3.2.2e[c]	*Individuals involved in training and their supervisors are identified.*
	3.2.2e[d]	*Practical exercises that are aligned with current threat scenarios are included in awareness training for **<ODP 3.2.2e[1]: roles>**.*
	3.2.2e[e]	*Feedback is provided to individuals involved in the training and their supervisors.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Awareness training policy; procedures addressing awareness training implementation; appropriate codes of federal regulations; awareness training curriculum; awareness training materials; security plan; training records; threat information on social engineering, advanced persistent threat actors, suspicious behaviors, breaches, or other relevant adversary tactics, techniques, or procedures; feedback on practical exercises and awareness training; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for awareness training; organizational personnel with information security responsibilities; organizational personnel with roles identified for practical exercises; supervisors of personnel with roles identified for practical exercises]. **Test**: [*SELECT FROM:* Automated mechanisms managing awareness training; automated mechanisms managing threat information].	

402

3.3 AUDIT AND ACCOUNTABILITY

There are no enhanced security requirements for audit and accountability.

3.4 CONFIGURATION MANAGEMENT

3.4.1e	**ENHANCED SECURITY REQUIREMENT** Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.4.1e[a]	*Approved system components are identified.*
	3.4.1e[b]	*Implemented system components are identified.*
	3.4.1e[c]	*An authoritative source and repository are established to provide a trusted source and accountability for approved and implemented system components.*
	3.4.1e[d]	*An authoritative source and repository are maintained to provide a trusted source and accountability for approved and implemented system components.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system and system component inventory records; inventory reviews and update records; security plan; system audit records; change control audit and review reports; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration management responsibilities; organizational personnel with responsibilities for system component inventory; organizational personnel with configuration change control responsibilities; organizational personnel with information security responsibilities; system/network administrators; members of change control board or similar]. **Test**: [*SELECT FROM:* Automated mechanisms that implement configuration change control; automated mechanisms supporting configuration control of the baseline configuration; automated mechanisms supporting and/or implementing the system component inventory].	

3.4.2e	**ENHANCED SECURITY REQUIREMENT** Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [*Selection (one or more): remove the components; place the components in a quarantine or remediation network*] to facilitate patching, re-configuration, or other mitigations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.4.2e[1]	***One or more of the following is/are selected: remove the components; place the components in a quarantine or remediation network.***
	3.4.2e[a]	*Misconfigured or unauthorized system components are detected.*
	3.4.2e[b]	*Automated mechanisms to detect misconfigured or unauthorized system components are identified.*

	3.4.2e[c]	*Automated mechanisms are employed to detect misconfigured or unauthorized system components.*
	3.4.2e[d]	*After detection, system components are* ***<ODP 3.4.2.e[1]: removed and/or placed in a quarantine or remediation network>*** *to facilitate patching, re-configuration, or other mitigations.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; procedures addressing system configuration change control; security plan; change control audit and review reports; agenda/minutes from configuration change control oversight meetings; alerts/notifications of unauthorized baseline configuration changes; system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration management responsibilities; organizational personnel with information security responsibilities; organizational personnel with configuration change control responsibilities; system developers; system/network administrators; members of change control board or similar roles]. **Test**: [*SELECT FROM:* Automated mechanisms supporting configuration control of the baseline configuration; automated mechanisms that implement security responses to changes to the baseline configurations; automated mechanisms that implement configuration change control; automated mechanisms that detect misconfigured or unauthorized system components].	

3.4.3e	**ENHANCED SECURITY REQUIREMENT** Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.4.3e[a]	*Automated discovery and management tools for inventory of system components are identified.*
	3.4.3e[b]	*Up-to-date, complete, accurate, and readily available inventory of system components exists.*
	3.4.3e[c]	*Automated discovery and management tools are employed to maintain an up-to-date, complete, accurate, and readily available inventory of system components.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing system component inventory; procedures addressing the baseline configuration of the system; configuration management plan; system design documentation; system architecture and configuration documentation; security plan; system configuration settings and associated documentation; configuration change control records; system inventory records; change control records; system maintenance records; system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information security responsibilities; organizational personnel with configuration management responsibilities; organizational personnel with responsibilities for managing the automated mechanisms implementing the system component inventory; system developers; system/network administrators]. **Test**: [*SELECT FROM:* Automated mechanisms implementing baseline configuration maintenance; automated mechanisms implementing the system component inventory].	

3.5 IDENTIFICATION AND AUTHENTICATION

3.5.1e	**ENHANCED SECURITY REQUIREMENT** Identify and authenticate [*Assignment: organization-defined systems and system components*] before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.5.1e[1]	***Systems and system components to identify and authenticate are defined.***
	3.5.1e[a]	*Bidirectional authentication that is cryptographically based is implemented.*
	3.5.1e[b]	*Bidirectional authentication that is replay resistant is implemented.*
	3.5.1e[c]	***<ODP-3.5.1e[1]: systems and system components>** are identified and authenticated before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing device identification and authentication; network connection policy; security plan; system configuration settings and associated documentation; system design documentation; list of devices requiring unique identification and authentication; device connection reports; system audit records; list of privileged system accounts; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system operations responsibilities; organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers]. **Test**: [*SELECT FROM:* Cryptographically-based bidirectional authentication mechanisms; automated mechanisms supporting and/or implementing network connection policy; automated mechanisms supporting and/or implementing replay resistant authentication mechanisms; automated mechanisms supporting and/or implementing identification and authentication capability; automated mechanisms supporting and/or implementing device identification and authentication capability].	

3.5.2e	**ENHANCED SECURITY REQUIREMENT** Employ automated mechanisms for the generation, protection, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.5.2e[a]	*Systems and system components that do not support multifactor authentication or complex account management are identified.*
	3.5.2e[b]	*Automated mechanisms for the generation, protection, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management are identified.*

	3.5.2e[c]	*Automated mechanisms for the generation, protection, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management are employed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; password policy; procedures addressing authenticator management; system design documentation; security plan; system configuration settings and associated documentation; list of system authenticator types; change control records associated with managing system authenticators; system audit records; password configurations and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information security responsibilities; organizational personnel with authenticator management responsibilities; system developers; system/network administrators]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing authenticator management capability].	

413
414

3.5.3e	**ENHANCED SECURITY REQUIREMENT** Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.5.3e[a]	*System components that are known, authenticated, in a properly configured state, or in a trust profile are identified.*
	3.5.3e[b]	*Automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems are identified.*
	3.5.3e[c]	*Automated or manual/procedural mechanisms are employed to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; identification and authentication policy; system and information integrity policy; procedures addressing system component inventory; procedures addressing device identification and authentication; procedures addressing device configuration management; procedures addressing system monitoring tools and techniques; configuration management plan; security plan; system design documentation; system configuration settings and associated documentation; system inventory records; configuration management records; system monitoring records; alerts/notifications of unauthorized components within the system; change control records; system audit records; system monitoring tools and techniques documentation; documented authorization/approval of network services; notifications or alerts of unauthorized network services; system monitoring logs or records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for managing the mechanisms implementing unauthorized system component detection; organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system/network administrators; organizational personnel with responsibility for monitoring the system; system developers].	

	Test: [*SELECT FROM:* Automated mechanisms implementing the detection of unauthorized system components; automated mechanisms supporting and/or implementing device identification and authentication capability; automated mechanisms for providing alerts; automated mechanisms supporting and/or implementing configuration management; cryptographic mechanisms supporting device attestation; automated mechanisms supporting and/or implementing system monitoring capability; automated mechanisms for auditing network services].

3.6 INCIDENT RESPONSE

3.6.1e	**ENHANCED SECURITY REQUIREMENT** Establish and maintain a security operations center capability that operates [*Assignment: organization-defined time period*].
	ASSESSMENT OBJECTIVE *Determine if:*

ODP 3.6.1e[1]	***A time period to operate a security operations center capability is defined.***
3.6.1e[a]	*A security operations center capability is established.*
3.6.1e[b]	*The security operations center capability operates* ***<ODP-3.6.1e[1]: time period>****.*
3.6.1e[c]	*The security operations center capability is maintained.*

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine: [*SELECT FROM:* Incident response policy; contingency planning policy; procedures addressing incident handling; procedures addressing the security operations center operations; automated mechanisms supporting dynamic response capabilities; incident response plan; contingency plan; security plan; other relevant documents or records].

Interview: [*SELECT FROM:* Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities; security operations center personnel; organizational personnel with information security responsibilities].

Test: [*SELECT FROM:* Automated mechanisms that support and/or implement the security operations center capability; automated mechanisms that support and/or implement the incident handling process].

3.6.2e	**ENHANCED SECURITY REQUIREMENT** Establish and maintain a cyber incident response team that can be deployed by the organization within [*Assignment: organization-defined time period*].
	ASSESSMENT OBJECTIVE *Determine if:*

ODP 3.6.2e[1]	***A time period for deploying a cyber incident response team is defined.***
3.6.2e[a]	*A cyber incident response team is established.*
3.6.2e[b]	*The cyber incident response team can be deployed by the organization within* ***<ODP-3.6.2e[1]: time period>****.*
3.6.2e[c]	*The cyber incident response team is maintained.*

	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident response; incident response plan; security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident response responsibilities; organizational personnel from the incident response team; organizational personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing incident response].

3.7 MAINTENANCE

There are no enhanced security requirements for maintenance.

3.8 MEDIA PROTECTION

There are no enhanced security requirements for media protection.

3.9 PERSONNEL SECURITY

3.9.1e	**ENHANCED SECURITY REQUIREMENT** Conduct [*Assignment: organization-defined enhanced personnel screening*] for individuals and reassess individual positions and access to CUI [*Assignment: organization-defined frequency*].
	ASSESSMENT OBJECTIVE *Determine if:*
	ODP 3.9.1e[1] — ***Enhanced personnel screening for individuals is defined.***
	ODP 3.9.1e[2] — ***The frequency to reassess individual positions and access to CUI is defined.***
	3.9.1e[a] — *Individuals that require enhanced personnel screening are identified.*
	3.9.1e[b] — *Positions that require access to CUI are identified.*
	3.9.1e[c] — ***<ODP-3.9.1e[1]: enhanced personnel screening>*** *is conducted for individuals.*
	3.9.1e[d] — *Individual positions and access to CUI is reassessed* ***<ODP-3.9.1e[2]: frequency>****.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Personnel security policy; system and services acquisition policy; records of screened personnel; procedures addressing personnel screening; security plan; list of appropriate access authorizations required by developers of the system; personnel screening criteria and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities; organizational personnel with system and services acquisition responsibilities; organizational personnel with responsibility for developer and personnel screening]. **Test**: [*SELECT FROM:* Organizational processes for personnel screening; organizational processes for developer screening; automated mechanisms supporting developer screening].

3.9.2e	**ENHANCED SECURITY REQUIREMENT** Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.9.2e[a]	*Individuals with access to CUI are identified.*
	3.9.2e[b]	*Organizational systems to which individuals have access are identified.*
	3.9.2e[c]	*Mechanisms are in place to protect organizational systems if adverse information develops or is obtained about individuals with access to CUI.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Personnel security policy; system and services acquisition policy; procedures addressing personnel screening; records of screened personnel; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; security plan; list of individuals who have been identified as posing an increased level of risk; list of appropriate access authorizations required for system personnel; personnel screening criteria and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities; organizational personnel with system and services acquisition responsibilities; organizational personnel with responsibility for personnel screening]. **Test**: [*SELECT FROM:* Organizational processes for personnel screening; automated mechanisms supporting personnel screening].	

3.10 PHYSICAL PROTECTION

There are no enhanced security requirements for physical protection.

3.11 RISK ASSESSMENT

3.11.1e	**ENHANCED SECURITY REQUIREMENT** Employ [*Assignment: organization-defined sources of threat intelligence*] as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.11.1e[1]	***Sources of threat intelligence are defined.***
	3.11.1e[a]	*A risk assessment methodology is identified.*
	3.11.1e[b]	***<ODP-3.11.1e[1]: sources of threat intelligence>*** *are employed as part of a risk assessment to guide and inform the development of organizational systems and security architectures, the selection of security solutions, and system monitoring, threat hunting, response, and recovery activities.*

	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Information security program plan; risk assessment policy; threat awareness program documentation; procedures for the threat awareness program; security planning policy and procedures; procedures addressing organizational assessments of risk; threat hunting program documentation; procedures for the threat hunting program; risk assessment results relevant to threat awareness; threat hunting results; list or other documentation on the cross-organization, information-sharing capability; security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; contingency planning policy; contingency plan; incident response policy; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel responsible for the threat awareness program; organizational personnel responsible for threat hunting program; organizational personnel with risk assessment responsibilities; organizational personnel with responsibility for the cross-organization, information sharing capability; organizational personnel with information security responsibilities; organizational personnel with contingency planning responsibilities; organizational personnel with incident response responsibilities; personnel with whom threat awareness information is shared by the organization]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing threat awareness program; automated mechanisms supporting and/or implementing the cross-organization, information-sharing capability; automated mechanisms supporting and/or implementing the threat hunting program; automated mechanisms for conducting, documenting, reviewing, disseminating, and updating risk assessments; automated mechanisms supporting and/or implementing contingency plans; automated mechanisms supporting and/or implementing incident response plans].

3.11.2e	**ENHANCED SECURITY REQUIREMENT** Conduct cyber threat hunting activities [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined event*]] to search for indicators of compromise in [*Assignment: organization-defined systems*] and detect, track, and disrupt threats that evade existing controls.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.11.2e[1]	***One or more of the following is/are selected: the frequency to conduct cyber threat hunting activities; the event triggering cyber threat hunting activities.***
	ODP 3.11.2e[2]	***The frequency to conduct cyber threat hunting activities is defined. (If selected in 3.11.2e[1])***
	ODP 3.11.2e[3]	***The event triggering cyber threat hunting activities is defined. (If selected in 3.11.2e[1])***
	ODP 3.11.2e[4]	***Organizational systems to search for indicators of compromise are defined.***
	3.11.2e[a]	*Cyber threat hunting activities are conducted* ***<ODP-3.11.2e[2] frequency*** *and/or* ***ODP-3.11.2e[3] event>*** *to search for indicators of compromise in* ***<OPD-3.11.2e[4]: systems>****.*
	3.11.2e[b]	*Cyber threat hunting activities are conducted* ***<ODP-3.11.2e[2] frequency*** *and/or* ***ODP-3.11.2e[3] event>*** *to detect, track, and disrupt threats that evade existing controls.*

	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and information integrity policy; policy and procedures addressing system monitoring; threat hunting program documentation; procedures for the threat hunting program; threat hunting results; system design documentation; security plan; system monitoring tools and techniques documentation; security planning policy and procedures; system configuration settings and associated documentation; system monitoring logs or records; system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel responsible for threat hunting program; system/network administrators; organizational personnel with information security responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel with responsibility for monitoring the system and/or network]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing threat hunting program; automated mechanisms supporting and/or implementing system monitoring capability; automated mechanisms supporting and/or implementing the discovery, collection, distribution, and use of indicators of compromise].

433
434

3.11.3e	**ENHANCED SECURITY REQUIREMENT** Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.11.3e[a] *Advanced automation and analytics capabilities to predict and identify risks to organizations, systems, and system components are identified.*
	3.11.3e[b] *Analysts to predict and identify risks to organizations, systems, and system components are identified.*
	3.11.3e[c] *Advanced automation and analytics capabilities are employed in support of analysts to predict and identify risks to organizations, systems, and system components.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and information integrity policy; risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; procedures addressing system monitoring; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system monitoring logs or records; system audit records; security plan; risk assessment artifacts; risk assessment results; risk assessment reviews; risk assessment updates; other relevant documents or records]. **Interview**: [*SELECT FROM:* organizational personnel with information security responsibilities; organizational personnel with risk assessment responsibilities; risk analysts; system developers; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel with responsibility for monitoring; system/network administrators]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing risk analytics capabilities; automated mechanisms supporting and/or implementing system monitoring capability; automated mechanisms supporting and/or implementing the discovery, collection, distribution, and use of indicators of compromise; automated mechanisms for conducting, documenting, reviewing, disseminating, and updating risk assessments].

435
436
437

3.11.4e	**ENHANCED SECURITY REQUIREMENT** Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.11.4e[a]	*The system security plan documents or references the security solution selected.*
	3.11.4e[b]	*The system security plan documents or references the rationale for the security solution.*
	3.11.4e[c]	*The system security plan documents or references the risk determination.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* system security plan; records of security plan reviews and updates; system design documentation; security planning policy; procedures addressing security plan development; procedures addressing security plan reviews and updates; enterprise architecture documentation; enterprise security architecture documentation; system interconnection security agreements and other information exchange agreements; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information security responsibilities; organizational personnel with responsibility for developing, implementing, or approving system interconnection and information exchange agreements; personnel managing the systems to which the Interconnection Security Agreement/Information Exchange Agreement applies; system developers; organizational personnel with security planning and plan implementation responsibilities; organizational personnel with boundary protection responsibilities; system developers; system/network administrators]. **Test**: [*SELECT FROM:* Organizational processes for security plan development, review, update, and approval].	

438
439

3.11.5e	**ENHANCED SECURITY REQUIREMENT** Assess the effectiveness of security solutions [*Assignment: organization-defined frequency*] to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.11.5e[1]	***The frequency to assess the effectiveness of security solutions is defined.***
	3.11.5e[a]	*Security solutions are identified.*
	3.11.5e[b]	*Current and accumulated threat intelligence is identified.*
	3.11.5e[c]	*Anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence is identified.*
	3.11.5e[d]	*The effectiveness of security solutions is assessed* ***<ODP-3.11.5e[1]: frequency>*** *to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Risk assessment policy; security planning policy and procedures; security assessment policy and procedures; security assessment plans; security assessment results; procedures addressing organizational assessments of risk; security plan; risk	

	assessment; risk assessment results; risk assessment reviews; risk assessment updates; threat intelligence information; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security assessment responsibilities; organizational personnel with risk assessment responsibilities; organizational personnel with threat analysis responsibilities; organizational personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms supporting, conducting, documenting, reviewing, disseminating, and updating risk assessments; automated mechanisms supporting and/or implementing security assessments].

3.11.6e	**ENHANCED SECURITY REQUIREMENT** Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.
	ASSESSMENT OBJECTIVE *Determine if:*
3.11.6e[a]	*Supply chain risks associated with organizational systems and system components are identified.*
3.11.6e[b]	*Supply chain risks associated with organizational systems and system components are assessed.*
3.11.6e[c]	*Supply chain risks associated with organizational systems and system components are responded to.*
3.11.6e[d]	*Supply chain risks associated with organizational systems and system components are monitored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing organizational assessments of risk; security planning policy and procedures; supply chain risk management plan; security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; threat intelligence information; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information security responsibilities organizational personnel with risk assessment responsibilities; organizational personnel with supply chain risk management responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms supporting, conducting, documenting, reviewing, disseminating, and updating risk assessments].

3.11.7e	**ENHANCED SECURITY REQUIREMENT** Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan [*Assignment: organization-defined frequency*].
	ASSESSMENT OBJECTIVE *Determine if:*
ODP 3.11.7e[1]	***The frequency for updating the supply chain risk management plan is defined.***
3.11.7e[a]	*Organizational systems and system components to include in a supply chain risk management plan are identified.*

	3.11.7e[b]	*A plan for managing supply chain risks associated with organizational systems and system components is developed.*
	3.11.7e[c]	*The plan for managing supply chain risks is updated* ***<OPD-3.11.7e[1]: frequency>****.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Risk assessment policy; supply chain risk management plan; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; threat intelligence information; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information security responsibilities; organizational personnel with risk assessment responsibilities; organizational personnel with supply chain risk management responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms supporting, conducting, documenting, reviewing, disseminating, and updating risk assessments].	

3.12 SECURITY ASSESSMENT

3.12.1e	**ENHANCED SECURITY REQUIREMENT** Conduct penetration testing [*Assignment: organization-defined frequency*], leveraging automated scanning tools and ad hoc tests using subject matter experts.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.12.1e[1]	***The frequency to conduct penetration testing is defined.***
	3.12.1e[a]	*Automated scanning tools are identified.*
	3.12.1e[b]	*Ad hoc tests using subject matter experts are identified.*
	3.12.1e[c]	*Penetration testing is conducted* ***<ODP-3.12.1e[1]: frequency>*** *leveraging automated scanning tools and ad hoc tests using subject matter experts.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security assessment policy; procedures addressing penetration testing; security plan; security assessment plan; penetration test report; security assessment report; security assessment evidence; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security assessment responsibilities; penetration testing team; system/network administrators; organizational personnel with information security responsibilities;]. **Test**: [*SELECT FROM:* Automated mechanisms supporting security assessments; automated mechanisms supporting penetration testing].	

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

3.13.1e	**ENHANCED SECURITY REQUIREMENT** Create diversity in [*Assignment: organization-defined system components*] to reduce the extent of malicious code propagation.

	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.13.1e[1]	***System components that require diversity are defined.***
	3.13.1e[a]	*Diversity in **<ODP-3.13.1e[1]: system components>** is created to reduce the extent of malicious code propagation.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security planning policy; procedures addressing information security architecture development; procedures addressing information security architecture reviews and updates; enterprise architecture documentation; information security architecture documentation; security plan; security CONOPS for the system; records of information security architecture reviews and updates; system and communications protection policy; system design documentation; system component inventory; list of technologies deployed in the system; acquisition documentation; acquisition contracts for system components or services; system audit records; system and services acquisition policy; enterprise architecture policy; procedures addressing developer security architecture and design specification for the system; solicitation documentation; service-level agreements; design specification and security architecture documentation for the system; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information security responsibilities; organizational personnel with information security architecture design and development responsibilities; organizational personnel with system acquisition, development, and implementation responsibilities; system/network administrators; system developers]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing the development, review, and update of the information security architecture; automated mechanisms supporting and/or implementing employment of a diverse set of information technologies].	

3.13.2e	**ENHANCED SECURITY REQUIREMENT** Implement the following changes to organizational systems and system components to introduce a degree of unpredictability into operations: [*Assignment: organization-defined changes and frequency of changes by system and system component*].	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.13.2e[1]	***Changes to organizational systems and system components to introduce a degree of unpredictability into operations are defined.***
	ODP 3.13.2e[2]	***The frequency of changes by system and system components is defined.***
	3.13.2e[a]	*Organizational systems and system components necessitating unpredictability are identified.*
	3.13.2e[b]	***<OPD-3.13.2e[1]: changes>** to organizational systems and system components are implemented **<OPD-3.13.2e[2]: frequency>** to introduce a degree of unpredictability into operations.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing concealment and misdirection techniques for the system; system design documentation; security plan; system configuration settings and associated documentation; system change control documentation; system architecture documentation; list of techniques to be employed to introduce randomness into organizational operations and assets; system audit records; other relevant documents or records].	

	Interview: [*SELECT FROM:* Organizational personnel with information security responsibilities; organizational personnel with change management responsibilities; organizational personnel with responsibility for implementing concealment and misdirection techniques for systems; system/network administrators]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing randomness as a concealment and misdirection technique; automated mechanisms supporting and/or implementing change control for the system].

3.13.3e	**ENHANCED SECURITY REQUIREMENT** Employ [*Assignment: organization-defined technical and procedural means*] to confuse and mislead adversaries.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.13.3e[1]	***Technical means to confuse and mislead adversaries are defined.***
	ODP 3.13.3e[2]	***Procedural means to confuse and mislead adversaries are defined.***
	3.13.3e[a]	***<ODP-3.13.3e[1]: technical means>*** *are employed to confuse and mislead adversaries.*
	3.13.3e[b]	***<ODP-3.13.3e[1]: procedural means>*** *are employed to confuse and mislead adversaries.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing concealment and misdirection techniques for the system; list of concealment and misdirection techniques to be employed for organizational systems; system design documentation; procedures addressing use of honeypots; security plan; system configuration settings and associated documentation; system design documentation; system architecture; list of techniques to be employed to introduce randomness into organizational operations and assets; system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information security responsibilities; system developers; system/network administrators; organizational personnel with responsibility for implementing concealment and misdirection techniques for systems]. **Test**: [*SELECT FROM:* Cryptographic mechanisms supporting and/or implementing concealment or randomization of communications patterns; automated mechanisms supporting and/or implementing alternative physical safeguards; automated mechanisms supporting and/or implementing honey pots; automated mechanisms supporting and/or implementing concealment and misdirection techniques].	

3.13.4e	**ENHANCED SECURITY REQUIREMENT** Employ [*Selection: (one or more):* [*Assignment: organization-defined physical isolation techniques*]; [*Assignment: organization-defined logical isolation techniques*]] in organizational systems and system components.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.13.4e[1]	***One or more of the following is/are selected: physical isolation techniques; logical isolation techniques.***

	ODP 3.13.4e[2]	***Physical isolation techniques are defined. (If selected in 3.13.4e[1])***
	ODP 3.13.4e[3]	***Logical isolation techniques are defined. (If selected in 3.13.4e[1])***
	3.13.4e[a]	***<ODP-3.13.4e[2]: physical isolation techniques*** *and/or* ***OPD-3.13.4e[3] logical isolation techniques>*** *are employed in organizational systems and system components.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; system design documentation; procedures addressing use of thin nodes; list of key internal boundaries of the system; security plan; boundary protection hardware and software; system configuration settings and associated documentation; enterprise architecture documentation; system architecture; security architecture documentation; system audit records; system component inventory; list of security tools and support components to be isolated from other system components; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with boundary protection responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing boundary protection capability; automated mechanisms implementing physical isolation techniques; automated mechanisms supporting and/or implementing isolation of information security tools, mechanisms, and support components; automated mechanisms supporting and/or implementing the capability to separate system components supporting organizational missions and business functions; automated mechanisms implementing logical isolation techniques; automated mechanisms supporting and/or implementing separate network addresses/different subnets; automated mechanisms supporting and/or implementing thin nodes].	

3.13.5e	**ENHANCED SECURITY REQUIREMENT** Distribute and relocate the following system functions or resources [*Assignment: organization-defined frequency*]: [*Assignment: organization-defined system functions or resources*].	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.13.5e[1]	***System functions or resources to distribute and relocate are defined.***
	ODP 3.13.5e[2]	***Frequency to distribute and relocate system functions or resources is defined.***
	3.13.5e[a]	***<ODP-3.13.5e[1]: system functions or resources>*** *are distributed and relocated* ***<ODP-3.13.5e[2]: frequency>****.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and communications protection policy; security plan; configuration management policy and procedures; procedures addressing concealment and misdirection techniques for the system; list of processing/storage locations to be changed at organizational time intervals; system component inventory; change control records; configuration management records; system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information security responsibilities; organizational personnel with responsibility for changing processing and/or storage locations; system/network administrators].	

	Test: [*SELECT FROM:* Automated mechanisms supporting and/or implementing changing processing and/or storage locations].

3.14 SYSTEM AND INFORMATION INTEGRITY

3.14.1e	**ENHANCED SECURITY REQUIREMENT** Verify the integrity of [*Assignment: organization-defined security critical or essential software*] using root of trust mechanisms or cryptographic signatures.
	ASSESSMENT OBJECTIVE *Determine if:*
	ODP 3.14.1e[1] — ***Security critical or essential software for verifying integrity is defined.***
	3.14.1e[a] — *Root of trust mechanisms or cryptographic signatures are identified.*
	3.14.1e[b] — *The integrity of* ***<ODP-3.14.1e[1]: security critical or essential software>*** *is verified using root of trust mechanisms or cryptographic signatures.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing software, firmware, and information integrity; system design documentation; security plan; system configuration settings and associated documentation; system component inventory; integrity verification tools and associated documentation; records of integrity verification scans; system audit records; cryptographic mechanisms and associated documentation; records of detected unauthorized changes to software, firmware, and information; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information security responsibilities; organizational personnel with responsibility for software, firmware, and/or information integrity; system developers; system/network administrators]. **Test**: [*SELECT FROM:* Software, firmware, and information integrity verification tools; automated mechanisms supporting and/or implementing integrity verification of the boot process; automated mechanisms supporting and/or implementing protection of the integrity of boot firmware; cryptographic mechanisms implementing software, firmware, and information integrity; safeguards implementing protection of the integrity of boot firmware].

3.14.2e	**ENHANCED SECURITY REQUIREMENT** Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.14.2e[a] — *Anomalous or suspicious behavior is defined.*
	3.14.2e[b] — *Organizational systems and system components are monitored on an ongoing basis for anomalous or suspicious behavior.*

	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; procedures addressing physical access monitoring; system design documentation; documentation providing evidence of correlated information obtained from audit records and physical access monitoring records; system configuration settings and associated documentation; procedures addressing system monitoring tools and techniques; system monitoring logs or records; system and information integrity policy; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system protocols; system audit records; security plan; system component inventory; records of actions taken to terminate suspicious events; alerts/notifications generated based on detected suspicious events; network diagram; system monitoring logs or records; list of profiles representing common traffic patterns and/or events; system protocols documentation; list of acceptable thresholds for false positives and false negatives; list of individuals who have been identified as posing an increased level of risk; list of privileged users; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with physical access monitoring responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel with responsibility for monitoring the system; organizational personnel with responsibility for the intrusion detection system]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing system monitoring capability; automated mechanisms supporting and/or implementing actions to terminate suspicious events; automated mechanisms supporting and/or implementing monitoring of inbound/outbound communications traffic; automated mechanisms implementing capability to correlate information from audit records with information from monitoring physical access; automated mechanisms supporting and/or implementing notifications to incident response personnel; automated mechanisms supporting and/or implementing analysis of outbound communications traffic; automated mechanisms supporting and/or implementing analysis of communications traffic/event patterns].

460
461

3.14.3e	**ENHANCED SECURITY REQUIREMENT** Ensure that [*Assignment: organization-defined systems and system components*] are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.
	ASSESSMENT OBJECTIVE *Determine if:*

ODP 3.14.3e[1]	***Systems and system components included in the scope of the specified enhanced security requirements are identified.***
3.14.3e[a]	***<ODP-3.14.3e[1]: systems and system components>*** *are included in the scope of the specified enhanced security requirements.*
3.14.3e[b]	*Systems and system components that are not included in* ***<ODP-3.14.3e[1]: systems and system components>*** *are segregated in purpose-specific networks.*

	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; information flow control policies; system and services acquisition policy; system and communications protection policy; procedures addressing security function isolation; procedures addressing application partitioning; procedures addressing security engineering principles used in the specification, design, development, implementation, and modification of the system; procedures addressing information flow enforcement; procedures addressing access enforcement; system architecture; system design documentation; security plan; system component inventory; system configuration settings and associated documentation; system configuration settings and associated documentation; system baseline configuration; list of security

	functions to be isolated from nonsecurity functions; system audit records; security requirements and specifications for the system; list of approved authorizations (user privileges); list of information flow authorizations; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; organizational personnel with acquisition/contracting responsibilities; system developers; system integrators; organizational personnel with responsibility for determining system security requirements; system security architects; enterprise architects; organizational personnel with system specification, design, development, implementation, and modification responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access control policy; automated mechanisms implementing information flow enforcement policy; automated mechanisms supporting the application of security engineering principles in system specification, design, development, implementation, and modification].

3.14.4e	**ENHANCED SECURITY REQUIREMENT** Refresh [*Assignment: organization-defined systems and system components*] from a known, trusted state [*Assignment: organization-defined frequency*].
	ASSESSMENT OBJECTIVE *Determine if:*
	ODP 3.14.4e[1] — ***Systems and system components to refresh from a known, trusted state are defined.***
	ODP 3.14.4e[2] — ***The frequency to refresh systems and systems components is defined.***
	3.14.4e[a] — *A known, trusted state is identified for* ***<ODP-3.14.4e[1]: systems and system components>***.
	3.14.4e[b] — ***<ODP-3.14.4e[1]: systems and system components>*** *are refreshed from a known, trusted state* ***<ODP-3.14.e[2]: frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing non-persistence for system components and information; system design documentation; security plan; system component inventory; system configuration settings and associated documentation; system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security responsibilities; organizational personnel with responsibility for non-persistence; system/network administrators; system developers]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing initiation and termination of non-persistent components; automated mechanisms supporting and/or implementing component and service refreshes].

3.14.5e	**ENHANCED SECURITY REQUIREMENT** Conduct reviews of persistent organizational storage locations [*Assignment: organization-defined frequency*] and remove CUI that is no longer needed.
	ASSESSMENT OBJECTIVE *Determine if:*
	ODP 3.14.5e[1] — ***The frequency with which to conduct reviews of persistent organizational storage locations is defined.***

	3.14.5e[a]	*Persistent organizational storage locations are identified.*
	3.14.5e[b]	*Reviews of persistent organizational storage locations are conducted* ***<ODP-3.14.5e[1]: frequency>*** *to identify CUI that is no longer needed.*
	3.14.5e[c]	*CUI that is no longer needed is removed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing protection of information at rest; system and information integrity policy; procedures addressing non-persistence for system components; system audit records; system design documentation; system configuration settings and associated documentation; security plan; cryptographic mechanisms and associated configuration documentation; offline storage locations for information at rest; system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* System/network administrators; system developers; organizational personnel with responsibility for non-persistence; organizational personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing removal of information from online storage; automated mechanisms supporting and/or implementing storage of information offline; automated mechanisms supporting and/or implementing initiation and termination of non-persistent components].	

3.14.6e	**ENHANCED SECURITY REQUIREMENT** Use threat indicator information and effective mitigations obtained from [*Assignment: organization-defined external organizations*] to guide and inform intrusion detection and threat hunting.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.14.6e[1]	***External organizations from which to obtain threat indicator information and effective mitigations are defined.***
	3.14.6e[a]	*Threat indicator information is identified.*
	3.14.6e[b]	*Effective mitigations are identified.*
	3.14.6e[c]	*Intrusion detection approaches are identified.*
	3.14.6e[d]	*Threat hunting activities are identified.*
	3.14.6e[e]	*Threat indicator information and effective mitigations obtained from* ***<ODP-3.14.6e[1]: external organizations>*** *are used to guide and inform intrusion detection and threat hunting.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and information integrity policy; information security program plan; procedures addressing security alerts, advisories, and directives; threat awareness program documentation; procedures addressing system monitoring; procedures for the threat awareness program; risk assessment results relevant to threat awareness; records of security alerts and advisories; system design documentation; security plan; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system monitoring logs or records; system audit records; documentation on the cross-organization information-sharing capability; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel responsible for the threat awareness program; organizational personnel with responsibility for the cross-organization information sharing capability; organizational personnel with information	

	security responsibilities; personnel with whom threat awareness information is shared by the organization; system/network administrators; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel with responsibility for monitoring system hosts; organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, and using the system; organizational personnel, organizational elements, and/or external organizations to whom alerts, advisories, and directives are to be disseminated; system developers]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing the threat awareness program; automated mechanisms supporting and/or implementing the cross-organization information-sharing capability; automated mechanisms supporting and/or implementing system monitoring capability; automated mechanisms supporting and/or implementing definition, receipt, generation, and dissemination of security alerts, advisories, and directives; automated mechanisms supporting and/or implementing security directives; automated mechanisms supporting and/or implementing threat hunting; automated mechanisms supporting and/or implementing intrusion detection; automated mechanisms supporting and/or implementing the discovery, collection, distribution, and use of indicators of compromise].

3.14.7e	**ENHANCED SECURITY REQUIREMENT** Verify the correctness of [*Assignment: organization-defined security critical or essential software, firmware, and hardware components*] using [*Assignment: organization-defined verification methods or techniques*].	
	ASSESSMENT OBJECTIVE *Determine if:*	
	ODP 3.14.7e[1]	***Security critical or essential software components for which to verify correctness are defined.***
	ODP 3.14.7e[2]	***Security critical or essential firmware components for which to verify correctness are defined.***
	ODP 3.14.7e[3]	***Security critical or essential hardware components for which to verify correctness are defined.***
	ODP 3.14.7e[4]	***Verification methods or techniques are defined.***
	3.14.7e[a]	*The correctness of* ***<ODP-3.14.7e[1]: security critical or essential software components>*** *is verified using* ***<ODP-3.14.7e[4]: verification methods or techniques>****.*
	3.14.7e[b]	*The correctness of* ***<ODP-3.14.7e[2]: security critical or essential firmware components>*** *is verified using* ***<ODP-3.14.7e[4]: verification methods or techniques>****.*
	3.14.7e[c]	*The correctness of* ***<ODP-3.14.7e[3]: security critical or essential hardware components>*** *is verified using* ***<ODP-3.14.7e[4]: verification methods or techniques>****.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and services acquisition policy; enterprise architecture policy; procedures addressing developer security architecture and design specification for the system; solicitation documentation; acquisition documentation; service-level agreements; acquisition contracts for the system, system component, or system service; design specification and security architecture documentation for the system; system design documentation; security plan; system component inventory; system configuration settings and associated documentation; other relevant documents or records].	

	Interview: [*SELECT FROM:* Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; system developers; organizational personnel with security architecture and design responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing integrity verification methods or techniques].

470
471

REFERENCES

LAWS, EXECUTIVE ORDERS, REGULATIONS, INSTRUCTIONS, STANDARDS, AND GUIDELINES[6]

LAWS AND EXECUTIVE ORDERS	
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283
[FOIA96]	Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. https://www.govinfo.gov/app/details/PLAW-104publ231
[44 USC 3502]	Title 44 U.S. Code, Sec. 3502, Definitions. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapI-sec3502
[44 USC 3552]	Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3552
[EO 13526]	Executive Order 13526 (2009) Classified National Security Information. (The White House, Washington, DC), DCPD-200901022, December 29, 2009. https://www.govinfo.gov/app/details/DCPD-200901022
[EO 13556]	Executive Order 13556 (2010) Controlled Unclassified Information. (The White House, Washington, DC), DCPD-201000942, November 4, 2010. https://www.govinfo.gov/app/details/DCPD-201000942
POLICIES, REGULATIONS, AND DIRECTIVES	
[32 CFR 2002]	32 CFR Part 2002, Controlled Unclassified Information, September 2016. https://www.govinfo.gov/app/details/CFR-2017-title32-vol6/CFR-2017-title32-vol6-part2002/summary
[OMB A-130]	Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[OMB M-19-03]	Office of Management and Budget (2018) Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program. (The White House, Washington, DC), OMB Memorandum M-19-03, December 10, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

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

[CNSSI 4009] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 4009. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

STANDARDS, GUIDELINES, AND REPORTS

[ISO 15408-1] International Organization for Standardization/International Electrotechnical Commission 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*, April 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[FIPS 140-3] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[FIPS 200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP 800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-53] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[SP 800-53A] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4

[SP 800-128] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128. https://doi.org/10.6028/NIST.SP.800-128

[SP 800-150] Johnson CS, Waltermire DA, Badger ML, Skorupka C, Snyder J (2016) Guide to Cyber Threat Information Sharing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-150. https://doi.org/10.6028/NIST.SP.800-150

[SP 800-160-2] Ross RS, Graubart R, Bodeau D, McQuaid R (2019) Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2. https://doi.org/10.6028/NIST.SP.800-160v2

[SP 800-171] Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2. https://doi.org/10.6028/NIST.SP.800-171r2

[SP 800-172] Ross RS, Pillitteri VY, Guissanie G, Wagner R, Graubart R, Bodeau (2021) Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-172. https://doi.org/10.6028/NIST.SP.800-172

MISCELLANEOUS PUBLICATIONS AND WEBSITES

[NARA CUI] National Archives and Records Administration (2019) *Controlled Unclassified Information (CUI) Registry*. https://www.archives.gov/cui

[Richards09] Richards MG, Hastings DE, Rhodes DH, Ross AM, Weigel AL (2009) Design for Survivability: Concept Generation and Evaluation in Dynamic Tradespace Exploration. *Second International Symposium on Engineering Systems* (Massachusetts Institute of Technology, Cambridge, MA). https://pdfs.semanticscholar.org/3734/7b58123c16e84e2f51a4e172ddee0a8755c0.pdf

474

475 APPENDIX A

476 # GLOSSARY

477 COMMON TERMS AND DEFINITIONS

478 Appendix A provides definitions for security terminology used within Special Publication
479 800-172A. Unless specifically defined in this glossary, all terms used in this publication are
480 consistent with the definitions contained in [CNSSI 4009] *National Information Assurance*
481 *Glossary*.

advanced persistent threat [SP 800-39]	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors including, for example, cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period; adapts to defenders' efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives.
agency [OMB A-130]	Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory 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 USC 3552]	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.
bidirectional authentication	Two parties authenticating each other at the same time. Also known as mutual authentication or two-way authentication.

boundary	Physical or logical perimeter of a system.
component	See *system component*.
confidentiality [44 USC 3552]	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 the 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 or functionality of the system.
controlled unclassified information [EO 13556]	Information that law, regulation, or government-wide 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 [32 CFR 2002]	Those types of information for which laws, regulations, or government-wide 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 [32 CFR 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 [32 CFR 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 [32 CFR 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.
cyber-physical system	Interacting digital, analog, physical, and human components engineered for function through integrated physics and logic.

cyber resiliency [SP 800-160-2]	The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.
damage-limiting operations	Procedural and operational measures that use system capabilities to maximize the ability of an organization to detect successful system compromises by an adversary and to limit the effects of such compromises (both detected and undetected).
defense-in-depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
designing for cyber resiliency and survivability	Designing systems, missions, and business functions to provide the capability to prepare for, withstand, recover from, and adapt to compromises of cyber resources in order to maximize mission or business operations.
dual authorization [CNSSI 4009, Adapted]	The system of storage and handling designed to prohibit individual access to certain resources by requiring the presence and actions of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.
enhanced security requirements	Security requirements that are to be implemented in addition to the basic and derived security requirements in NIST Special Publication 800-171. The additional security requirements provide the foundation for a defense-in-depth protection strategy that includes three mutually supportive and reinforcing components: (1) penetration-resistant architecture, (2) damage-limiting operations, and (3) designing for cyber resiliency and survivability.
environment of operation [SP 800-37, Adapted]	The physical surroundings in which a system processes, stores, and transmits information.
executive agency [OMB A-130]	An executive department specified in 5 U.S.C. Sec. 101; a military department specified in 5 U.S.C. Sec. 102; an independent establishment as defined in 5 U.S.C. Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C. Chapter 91.
federal agency	See *executive agency*.
firmware	Computer programs and data stored in hardware—typically in read-only memory (ROM) or programmable read-only memory (PROM)—such that programs and data cannot be dynamically written or modified during execution of the programs. See *hardware* and *software*.
hardware	The material physical components of a system. See *software* and *firmware*.

high-value asset [OMB M-19-03]	A designation of federal information or a federal information system when it relates to one or more of the following categories: - *Informational Value* – The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries. - *Mission Essential* – The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEF), as approved in accordance with Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system. - *Federal Civilian Enterprise Essential (FCEE)* – The information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.
impact	With respect to security, 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. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.
incident [44 USC 3552]	An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
information [OMB A-130]	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.
information flow control	Procedure to ensure that information transfers within a system are not made in violation of the security policy.
information resources [44 USC 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
information security [44 USC 3552]	The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
information system [44 USC 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
information technology [OMB A-130]	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment that are used in the automatic

	acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.
integrity [44 USC 3552]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
internet of things	The network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information.
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.
misdirection	The process of maintaining and employing deception resources or environments and directing adversary activities to those resources or environments.
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 *authenticator*.

mutual authentication	The process of both entities involved in a transaction verifying each other. See *bidirectional authentication*.
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.
organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure.
penetration-resistant architecture	An architecture that uses technology and procedures to limit the opportunities for an adversary to compromise an organizational system and to achieve a persistent presence in the system.
personnel security [SP 800-53]	The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities requiring trustworthiness.
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 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).
risk [OMB A-130]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
risk assessment [SP 800-30]	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.
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.

security	A condition that results from the establishment and maintenance of protective measures that enable an organization 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 organization's risk management approach.
security assessment	See *security control assessment*.
security control [OMB A-130]	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
security control assessment [OMB A-130]	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 an information system or organization.
security domain [CNSSI 4009, Adapted]	A domain that implements a security policy and is administered by a single authority.
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 solution	The key design, architectural, and implementation choices made by organizations in satisfying specified security requirements for systems or system components.
survivability [Richards09]	The ability of a system to minimize the impact of a finite-duration disturbance on value delivery (i.e., stakeholder benefit at cost), achieved through the reduction of the likelihood or magnitude of a disturbance; the satisfaction of a minimally acceptable level of value delivery during and after a disturbance; and/or a timely recovery.
system	See *information system*.
system component [SP 800-128]	A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.
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 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.

tactics, techniques, and procedures [SP 800-150]	The behavior of an actor. A tactic is the highest-level description of the behavior; techniques provide a more detailed description of the behavior in the context of a tactic; and procedures provide a lower-level, highly detailed description of the behavior in the context of a technique.
threat [SP 800-30]	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.
threat information [SP 800-150]	Any information related to a threat that might help an organization protect itself against the threat or detect the activities of an actor. Major types of threat information include indicators, TTPs, security alerts, threat intelligence reports, and tool configurations.
threat intelligence [SP 800-150]	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.
situational awareness [CNSSI 4009]	Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.
user [CNSSI 4009, Adapted]	Individual, or (system) process acting on behalf of an individual, authorized to access a system.

482

483 **APPENDIX B**

484 # ACRONYMS

485 COMMON ABBREVIATIONS

APT	Advanced Persistent Threat
CFR	Code of Federal Regulations
CNSS	Committee on National Security Systems
CUI	Controlled Unclassified Information
EO	Executive Order
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOIA	Freedom Of Information Act
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISOO	Information Security Oversight Office
IT	Information Technology
ITL	Information Technology Laboratory
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
OMB	Office of Management and Budget
ODP	Organization-defined Parameter
SP	Special Publication
USC	United States Code

486

APPENDIX C

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 [SP 800-172]: *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 C-1 through C-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.

510 **TABLE C-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.[7] **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**.

[7] 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.[8]	
		Basic	Examination that uses a representative sample of assessment objects (by type and number within type) to provide the 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 the 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 the 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 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.		

511

[8] 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.

512 **TABLE C-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.[9]	
		Basic	Interview that uses a representative sample of individuals in organizational roles to provide the level of coverage necessary for determining whether the security safeguards are implemented and free of obvious errors.

513

[9] 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 the 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 the 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 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.		

514

515 **TABLE C-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.[10]			
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.		

516

[10] 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 (e.g., penetration testing).

		Basic	Testing that uses a representative sample of assessment objects by type and number within type, to provide the 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 the 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 the 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 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 a vulnerability scanning capability.		

517
518