NIST Special Publication 800
NIST SP 800-172Ar3 ipd

Assessing Enhanced Security Requirements for Controlled Unclassified Information

Initial Public Draft

Ron Ross
Victoria Pillitteri

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-172Ar3.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800
NIST SP 800-172Ar3 ipd

Assessing Enhanced Security Requirements for Controlled Unclassified Information

Initial Public Draft

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-172Ar3.ipd

September 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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 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 all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority
This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283 [1]. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130 [2].

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

How to Cite this NIST Technical Series Publication:
Ross R, Pillitteri V (2025) Assessing Enhanced Security Requirements for Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-172Ar3 ipd. https://doi.org/10.6028/NIST.SP.800-172Ar3.ipd

Author ORCID iDs
Ron Ross: 0000-0002-1099-9757
Victoria Pillitteri: 0000-0002-7446-7506

Public Comment Period
September 29, 2025 – November 14, 2025

Submit Comments
800-171comments@list.nist.gov
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments submitted during the public comment period will be posted to the NIST Protecting Controlled Unclassified Information Project page. with contact information redacted. All technical content will be posted as submitted, so commenters should not include information they do not wish to be posted (e.g., personal or business information).

Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/172/A/r3/ipd, including related content, potential updates, and document history.

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

Abstract

The protection of controlled unclassified information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully conduct its essential missions and functions. This publication provides federal agencies with assessment procedures for the security requirements in NIST SP 800-172. The assessment procedures are flexible and can be tailored to the needs of federal agencies and assessors. Security requirement 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 federal agency-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 security requirements.

Keywords

assessment; assessment procedure; assurance; enhanced security requirement; enhanced security requirement assessment; controlled unclassified information; Executive Order 13556; nonfederal organization; nonfederal system; security assessment.

Reports on Computer Systems Technology

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

Audience

This publication serves a diverse group of individuals and organizations in the public and private sectors, including individuals with:

- System development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, system/security engineers, systems integrators)
- Acquisition or procurement responsibilities (e.g., contracting officers)
- System, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers)
- Security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts)

The above roles and responsibilities can be viewed from two perspectives:

- *Federal perspective*: The entity establishing and conveying security assessment requirements in contractual vehicles or other types of agreements
- *Nonfederal perspective*: The entity responding to and complying with the security assessment requirements set forth in contracts or agreements

Note to Reviewers

The following significant changes have been made in the initial public draft (ipd) of SP 800-172Ar3 (Revision 3):

- The restructuring of the assessment procedure syntax to align with SP 800-53A [5]
- The addition of assessment procedures for the new and revised enhanced security requirements in draft SP 800-172r3 [3]
- The addition of a references section to provide source assessment procedures from SP 800-53A [5]
- A one-time change to the publication version number to align with SP 800-172, Revision 3 [3]

NIST is specifically interested in comments, feedback, and recommendations on the following topics:

- The alignment of the assessment procedures to SP 800-53A [5]
- The ease-of-use of the assessment procedures in conducting assessments of the CUI enhanced security requirements
- The usefulness of the information in supplementary Appendices C, D, and E

Reviewers are encouraged to comment on all or parts of SP 800-172Ar3 ipd. NIST requests that all comments be submitted to 800-171comments@list.nist.gov by 11:59 p.m. Eastern Standard Time (EST) on November 14, 2025. Commenters are encouraged to use the comment template provided with the document announcement.

Comments received in response to this request will be posted on the Protecting CUI project site after the due date. Submitters' names and affiliations (when provided) will be included, while contact information will be removed.

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 also 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: 800-171comments@list.nist.gov

Table of Contents

List of Tables

Acknowledgments

The authors gratefully acknowledge and appreciate the contributions from individuals and organizations in the public and private sectors whose constructive comments improved the overall quality, thoroughness, and usefulness of this publication. The authors also wish to thank the NIST technical editing and production staff — Jim Foti, Jeff Brewer, Eduardo Takamura, Jeremy Licata, Isabel Van Wyk, and Cristina Ritfeld — for their outstanding support in preparing this document for publication.

1. Introduction

The security assessment process gathers information and produces evidence to determine the effectiveness of security requirements by:

- Identifying potential problems or shortfalls in security and risk management programs
- Identifying security weaknesses and deficiencies in systems and the environments in which those systems operate
- Prioritizing risk mitigation decisions and activities
- Confirming that identified security weaknesses and deficiencies in the system and environment of operation have been addressed
- Supporting continuous monitoring activities and providing information security situational awareness

1.1. Purpose and Applicability

The purpose of this publication is to provide procedures for assessing the security requirements in NIST Special Publication (SP) 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information* [3]. Organizations can use the assessment procedures to generate evidence that the security requirements have been satisfied. The scope of the security assessments conducted using the procedures described in this publication is guided and informed by the system security plans for systems that process, store, or transmit CUI. The assessment procedures 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]

1.2. Organization of This Publication

The remainder of this special publication is organized as follows:

- Section 2 describes the fundamental concepts associated with assessments of security requirements, including assessment procedures, methods, objects, and assurance cases that can be created using the evidence produced during assessments. This section mirrors the material included SP 800-171A, Sec. 2, with minor updates to reflect the enhanced security requirements and assessment procedures.
- Section 3 provides assessment procedures for the security requirements in SP 800-172 [3], including assessment objectives and potential assessment methods and objects for each procedure.

[1] The term *risk* refers to risks to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. See SP 800-39 [4] for additional information on organizational risk management and risk tolerance.

175 The following sections provide additional information to support the assessment of security
176 requirements for the protection of CUI:

177 • References
178 • Appendix A: Acronyms
179 • Appendix B: Glossary
180 • Appendix C: Summary of Enhanced Security Requirements
181 • Appendix D: Security Requirement Assessments
182 • Appendix E: Organization-Defined Parameters
183 • Appendix F: Change Log

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

184

2. The Fundamentals

The process used by organizations and assessors to assess the security requirements in SP 800-172 [3] includes (1) preparing for the assessment, (2) developing a security assessment plan, (3) conducting the assessment, and (4) documenting, analyzing, and reporting the assessment results. The remainder of this section describes the structure and content of the procedures used to assess the security requirements and the importance of assurance cases in providing the evidence necessary to determine compliance with the requirements.

2.1. Assessment Procedures

The enhanced security requirements in SP 800-172 [3] are organized into 17 families, as illustrated in Table 1.

Table 1. Enhanced security requirement families

Access Control	Maintenance	Security Assessment and Monitoring
Awareness and Training	Media Protection	System and Communications Protection
Audit and Accountability	Personnel Security	System and Information Integrity
Configuration Management	Physical Protection	Planning
Identification and Authentication	Risk Assessment	System and Services Acquisition
Incident Response		Supply Chain Risk Management

The assessment procedures in Sec. 3 are grouped by similar family designations to ensure the completeness and consistency of assessments. The procedures have been derived from and are sourced to the assessment procedures in SP 800-53A [5].

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 potential assessment objective includes a determination statement related to the security requirement. If there is an organization-defined parameter (ODP) in the security requirement, then the assessment objective begins with a determination statement related to the definition of the ODP. The determination statements are linked to the content of the security requirements to help ensure traceability of the assessment results to the requirements.

Assessment objects identify the specific items being assessed and can include specifications, mechanisms, activities, and individuals. Specifications are the documented artifacts[2] (e.g., plans, policies, procedures, requirements, functional and assurance specifications, design documentation, architectures) associated with a system. Mechanisms are the hardware, software, and firmware safeguards implemented within a system. Activities are the protection-related actions supporting a system that involve people (e.g., conducting system backup

[2] Artifacts may be in formats other than documents (e.g., databases; Governance, Risk, and Compliance [GRC] tools; Open Security Controls Assessment Language [OSCAL]).

operations, exercising an incident response plan, monitoring network traffic). Individuals are the people applying the specifications, mechanisms, or activities described above.

Assessment methods define the nature and extent of the assessor's actions and are used to facilitate understanding, achieve clarification, or obtain evidence. The assessment methods include *examine*, *interview*, and *test*. The examine method is the process of reviewing, studying, inspecting, or analyzing assessment objects. The interview method is the process of holding discussions with individuals or groups about assessment objects. The test method is the process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior. Assessment methods include attributes of *depth* and *coverage*, which define the rigor, scope, and level of effort for the assessment as well as the degree of assurance that the security requirements have been satisfied. See SP 800-53A, Appendix D [5].

The structure and content of an assessment procedure are provided in the example below.

03.01.01E Dual Authorization — **Security Requirement Name**

ASSESSMENT OBJECTIVE

Determine if: — **Determination Statement for Security Requirement**

A.03.01.01E.ODP[01]: *privileged commands and/or other actions requiring dual authorization are defined*.

A.03.01.01E: dual authorization is enforced for ***<A.03.01.01E.ODP[01]: privileged commands and/or other actions>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; procedures addressing access enforcement and dual authorization; system design documentation; system configuration settings and associated documentation; list of actions requiring dual authorization; list of privileged commands requiring dual authorization; list of approved authorizations (user privileges); system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with access enforcement responsibilities; system/network administrators; system personnel with information security responsibilities].

Test

[SELECT FROM: Dual authorization mechanisms implementing access control policy].

REFERENCES

Source Assessment Procedures: AC-03(02)

Determination statements have alphanumeric identifiers. Each determination statement begins with the letter "**A**" to indicate that it is part of an assessment procedure. The next sequence of numbers followed by the letter "**E**" indicates the enhanced security requirement identifier from SP 800-172 [3] (and the specific control item if it is a multi-part requirement) that is the target of the assessment. Organization-defined parameters are indicated by the letters "**ODP**." If there are multiple ODPs in the determination statement, the ODP number is indicated in a square bracket (e.g., **A.03.01.04E.ODP[01]**). Square brackets are also used to denote when an assessment procedure further decomposes a requirement into more granular determination statements (e.g., **A.03.10.03E.a[01]**, **A.03.10.03E.a[02]**, **A.03.10.03E.a[03]**, **A.03.10.03E.a[04]**).

The application of an assessment procedure to a security requirement produces assessment results or *findings*. The findings are compiled and used as evidence to determine whether the security requirement has been *satisfied* or *other than satisfied*. A finding of satisfied indicates that the assessment objective has been met, producing a fully acceptable result. A finding of other than satisfied indicates that there are potential anomalies that may need to be addressed by the organization. A finding of other than satisfied may also indicate that the assessor was unable to obtain sufficient information to make the specific determination called for in the determination statement.

2.2. Assurance Cases

Building an effective assurance case to determine compliance with security requirements involves compiling evidence from a variety of sources and conducting different types of activities during an assessment. An *assurance case* is a body of evidence organized into an argument demonstrating that some claim about a system is true. For security assessments conducted using the procedures in this publication, that claim is "compliance" with the security requirements in SP 800-172 [3]. Assessors obtain evidence during security assessments to allow designated officials[3] to make objective determinations about compliance with the security requirements. The evidence needed to make such determinations can be obtained from various sources, including independent, third-party assessments or other types of assessments, depending on the needs of the organization establishing the requirements and the organization conducting the assessments.

For example, many technical security requirements are satisfied by security capabilities that are built into commercial information technology products and systems. Product assessments are typically conducted by independent, third-party testing organizations.[4] These assessments examine the security functions of products and established configuration settings. Assessments can also be conducted to demonstrate compliance with 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

[3] A *designated official* is either internal or external to a nonfederal organization and has the responsibility to determine organizational compliance with the security requirements.

[4] Examples of third-party testing organizations include Common Criteria Testing Laboratories that evaluate IT products in accordance with ISO/IEC 15408 [6] and Cryptographic Module Validation Program Testing Laboratories that evaluate cryptographic modules in accordance with Federal Information Processing Standards (FIPS) 140 [7].

hundreds of thousands of systems, these types of assessments can be carried out at a greater level of depth and provide deeper insights into the security capabilities of the products.

The evidence needed to determine compliance with the security requirements is obtained by assessing the implementation of the safeguards and countermeasures selected to satisfy the requirements. Assessors can build on previously developed materials that started with the specification of the information security needs of the organization and were further improved during the design, development, and implementation of the system. These materials provide the initial evidence for an assurance case.

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

The assessment procedures in this publication are based on and sourced to the assessment procedures in SP 800-53A [5]. For additional information and guidance on preparing for security assessments, developing assessment plans, conducting assessments, and analyzing assessment report results, consult SP 800-53A [5].

3. The Procedures

This section provides assessment procedures for the security requirements defined in SP 800-172 [3]. Organizations that conduct security requirement assessments can develop their security assessment plans by using the information provided in the assessment procedures and selecting the specific POTENTIAL ASSESSMENT METHODS AND OBJECTS that meet the organization's needs. Organizations also have flexibility in defining the level of rigor and detail associated with the assessment based on the assurance requirements of the organization.

3.1. Access Control

03.01.01E Dual Authorization

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.01E.ODP[01]: *privileged commands and/or other actions requiring dual authorization are defined*.

A.03.01.01E: dual authorization is enforced for ***<A.03.01.01E.ODP[01]: privileged commands and/or other actions>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; procedures addressing access enforcement and dual authorization; system design documentation; system configuration settings and associated documentation; list of actions requiring dual authorization; list of privileged commands requiring dual authorization; list of approved authorizations (user privileges); system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with access enforcement responsibilities; system/network administrators; system developers; personnel with information security responsibilities].

Test

[SELECT FROM: Dual authorization mechanisms implementing access control policy].

REFERENCES

Source Assessment Procedures: AC-03(02)

03.01.02E Non-Organizationally Owned Systems - Restricted Use

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.02E.ODP[01]: *restrictions on the use of non-organizationally owned systems or system components to process, store, or transmit CUI are defined*.

A.03.01.02E: the use of non-organizationally owned systems or system components to process, store, or transmit CUI is restricted using ***<A.03.01.02E.ODP[01]: restrictions>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; procedures addressing the use of external systems; system design documentation; system configuration settings and associated documentation; system connection or processing agreements; account management documents; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for restricting or prohibiting the use of non-organizationally owned systems, system components, or devices; system/network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms implementing restrictions on the use of non-organizationally owned systems, components, or devices].

REFERENCES

Source Assessment Procedures: AC-20(03)

03.01.03E Withdrawn

Addressed by 03.01.09E, 03.01.10E, and 03.01.03.

03.01.04E Concurrent Session Control

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.04E.ODP[01]: *accounts and/or account types for which to limit the number of concurrent sessions is defined*.

A.03.01.04E.ODP[02]: *the number of concurrent sessions to be allowed for each account and/or account type is defined*.

A.03.01.04E: the number of concurrent sessions for each ***<A.03.01.04E.ODP[01]: account and/or account types>*** is limited to ***<A.03.01.04E.ODP[02]: number>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; procedures addressing concurrent session control; system design documentation; system configuration settings and associated documentation; security plan; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing access control policy for concurrent session control].

REFERENCES

Source Assessment Procedures: AC-10

03.01.05E Remote Access Monitoring and Control

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.05E[01]: automated mechanisms are employed to monitor remote access methods.

A.03.01.05E[02]: automated mechanisms are employed to control remote access methods.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; procedures addressing remote access to the system; system design documentation; system configuration settings and associated documentation; system audit records; system monitoring records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Automated mechanisms monitoring and controlling remote access methods].

REFERENCES

Source Assessment Procedures: AC-17(01)

03.01.06E Protection of Remote Access Mechanism Information

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.06E: information about remote access mechanisms is protected from unauthorized use and disclosure.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; procedures addressing remote access to the system; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for implementing or monitoring remote access to the system; system users with knowledge of information about remote access mechanisms; personnel with information security responsibilities].

REFERENCES

Source Assessment Procedures: AC-17(06)

03.01.07E Automated Audit Actions for Account Management

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.07E[01]: automated mechanisms are used to audit account creation actions.

A.03.01.07E[02]: automated mechanisms are used to audit account modification actions.

A.03.01.07E[03]: automated mechanisms are used to audit account enabling actions.

A.03.01.07E[04]: automated mechanisms are used to audit account disabling actions.

A.03.01.07E[05]: automated mechanisms are used to audit account removal actions.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; notifications or alerts of account creation, modification, enabling, disabling, and removal actions; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with account management responsibilities; system/network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Automated mechanisms implementing account management functions].

REFERENCES

Source Assessment Procedures: AC-02(04)

03.01.08E Account Monitoring for Atypical Usage

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.08E.ODP[01]: ***atypical usage for which to monitor system accounts is defined.***

A.03.01.08E.ODP[02]: ***personnel or roles to report atypical usage are defined.***

A.03.01.08E.a: system accounts are monitored for ***<A.03.01.08E.ODP[01]: atypical usage>***.

A.03.01.08E.b: atypical usage of system accounts is reported to ***<A.03.01.08E.ODP[02]: personnel or roles>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated

documentation; system monitoring records; system audit records; audit tracking and monitoring reports; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with account management responsibilities; system/network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms implementing account management functions].

REFERENCES

Source Assessment Procedure: AC-02(12)

03.01.09E Attribute-Based Access Control

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.09E.ODP[01]: *attributes to assume access permissions are defined*.

A.03.01.09E.a[01]: the attribute-based access control policy is enforced over defined subjects.

A.03.01.09E.a[02]: the attribute-based access control policy is enforced over defined objects.

A.03.01.09E.b: access is controlled based upon ***<A.03.01.09E.ODP[01]: attributes>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of subjects and objects (i.e., users and resources) requiring enforcement of attribute-based access control policies; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with access enforcement responsibilities; system/network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms implementing access enforcement functions].

REFERENCES

Source Assessment Procedures: AC-03(13)

03.01.10E Object Security Attributes

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.10E.ODP[01]: ***security attributes to be associated with information, source, and destination objects are defined.***

A.03.01.10E.ODP[02]: ***information objects to be associated with information security attributes are defined.***

A.03.01.10E.ODP[03]: ***source objects to be associated with information security attributes are defined.***

A.03.01.10E.ODP[04]: ***destination objects to be associated with information security attributes are defined.***

A.03.01.10E.ODP[05]: ***information flow control policies as a basis for the enforcement of flow control decisions are defined.***

A.03.01.10E: ***<A.03.01.10E.ODP[01]: security attributes>*** associated with ***<A.03.01.10E.ODP[02]: information objects>***, ***<A.03.01.10E.ODP[03]: source objects>***, and ***<A.03.01.10E.ODP[04]: destination objects>*** are used to enforce ***<A.03.01.10E.ODP[05]: information flow control policies>*** as a basis for flow control decisions.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of security attributes and associated source and destination objects; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing information flow enforcement policy].

REFERENCES

Source Assessment Procedure: AC-04(01)

03.01.11E Role-Based Access Control

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.11E.ODP[01]: roles and users authorized to assume such roles are defined.

A.03.01.11E.a: a role-based access control policy over defined subjects and objects is enforced.

A.03.01.11E.b: access is controlled based upon **<A.03.01.11E.ODP[01] roles and authorized users>**.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; role-based access control policies; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of roles, users, and associated privileges required to control system access; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing role-based access control policy].

REFERENCES

Source Assessment Procedure: AC-03(07)

03.01.12E Physical or Logical Separation of CUI Flows

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.12E.ODP[01]: mechanisms and/or techniques to separate CUI flows are defined.

A.03.01.12E: CUI flows are logically or physically separated using **<A.03.01.12E.ODP[01] mechanisms and/or techniques>.**

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Information flow enforcement policy; information flow control

policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of required separation of information flows by information types; list of mechanisms and/or techniques used to logically or physically separate information flows; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing information flow enforcement functions].

REFERENCES

Source Assessment Procedure: AC-04(21)

03.01.13E Metadata

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.13E.ODP[01]: metadata on which to base enforcement of information flow control is defined.

A.03.01.13E: information flow control based on **<A.03.01.13E.ODP[01]: metadata>** is enforced.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing information flow enforcement policy].

REFERENCES

Source Assessment Procedure: AC-04(06)

03.01.14E Security Policy Filters

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.14E.ODP[01]: security policy filters are defined.

A.03.01.14E.ODP[02]: information flows are defined.

A.03.01.14E.ODP[03]: one or more of the following PARAMETER VALUES is/are selected: {Block; Strip; Modify; Quarantine} in response to a filter processing failure.

A.03.01.14E.ODP[04]: security policy addressing a filter processing failure is defined.

A.03.01.14E.a: information flow control is enforced using **<A.03.01.14E.ODP[01] security policy filters>** as a basis for flow control decisions **for <A.03.01.14E.ODP[02] information flows>**.

A.03.01.14E.b: <A.03.01.14E.ODP[03]: SELECTED PARAMETER VALUE(S)> data after a filter processing failure in accordance with **<A.03.01.14E.ODP[04] security policy>.**

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of security policy filters regulating flow control decisions; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing information flow enforcement policy; security policy filters].

REFERENCES

Source Assessment Procedure: AC-04(08)

03.01.15E Data Type Identifiers

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.15E.ODP[01]: data type identifiers are defined.

A.03.01.15E: when transferring information between security domains, **<A.03.01.15E.ODP[01]: data type identifiers>** are used to validate data that is essential for information flow decisions.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of data type identifiers; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing information flow enforcement policy].

REFERENCES

Source Assessment Procedure: AC-04(12)

03.01.16E Decomposition Into Policy-Relevant Subcomponents

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.16E.ODP[01]: policy-relevant subcomponents into which to decompose CUI for submission to policy enforcement mechanisms are defined.

A.03.01.16E: when transferring information between different security domains, CUI is decomposed into **<A.03.01.16E.ODP[01]: policy-relevant subcomponents>** for submission to policy enforcement mechanisms

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing information flow enforcement policy].

REFERENCES

Source Assessment Procedure: AC-04(13)

03.01.17E Detection of Unsanctioned CUI

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.17E.ODP[01]: unsanctioned CUI to be detected is defined.

A.03.01.17E.ODP[02]: a security policy that prohibits the transfer of unsanctioned information is defined.

A.03.01.17E.a: when transferring information between different security domains, information is examined for the presence of **<A.03.01.17E.ODP[01] unsanctioned information>**.

A.03.01.17E.b: the transfer of CUI defined in 03.01.17E.a is prohibited in accordance with **<A.03.01.17E.ODP[02] security policy>**.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of unsanctioned information types and associated information; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing information flow enforcement policy].

REFERENCES

Source Assessment Procedure: AC-04(15)

3.2. Awareness and Training

03.02.01E Advanced Literacy and Awareness Training

ASSESSMENT OBJECTIVE

Determine if:

A.03.02.01E.ODP[01]: ***indicators of malicious code are defined.***

A.03.02.01E.ODP[02]: ***the frequency at which to update security literacy training content is defined.***

A.03.02.01E.ODP[03]: ***events which cause security literacy training content to be updated are defined.***

A.03.02.01E.a.01: security literacy training on the advanced persistent threat is provided.

A.03.02.01E.a.02: security literacy training on recognizing suspicious communications and anomalous behavior in systems using ***<A.03.02.01E.ODP[01]: indicators of malicious code>*** is provided.

A.03.02.01E.a.03: security literacy training on the cyber threat environment is provided.

A.03.02.01E.b: security literacy training content is updated ***<A.03.02.01E.ODP[02]: frequency>*** and following ***<A.03.02.01E.ODP[03]: events>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System security plan; security literacy and awareness training policy; procedures addressing security literacy and awareness training implementation; security literacy and awareness training curriculum; security literacy and awareness training materials; other relevant documents or records].

Interview

[SELECT FROM: Personnel who receive security literacy and awareness training; personnel with responsibilities for security literacy and awareness training; personnel with information security responsibilities].

REFERENCES

Source Assessment Procedures: AT-02(04), AT-02(05), AT-02(06)

03.02.02E Literacy and Awareness Training Practical Exercises

ASSESSMENT OBJECTIVE

Determine if:

A.03.02.02E: practical exercises in literacy training that simulate events and incidents are provided.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System security plan; security literacy and awareness training policy; procedures addressing security literacy and awareness training implementation; security awareness training curriculum; security awareness training materials; other relevant documents or records].

Interview

[SELECT FROM: Personnel who receive security literacy and awareness training; personnel with responsibilities for security awareness training; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms implementing cyber-attack simulations in practical exercises].

REFERENCES

Source Assessment Procedures: AT-02(01)

03.02.03E Literacy and Awareness Training Feedback

ASSESSMENT OBJECTIVE

Determine if:

A.03.02.03E.ODP[01]: ***personnel to whom feedback on organizational training results will be provided are assigned.***

A.03.02.03E: feedback on organizational training results is provided to ***<A.03.02.03E.ODP[01]: personnel>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Security awareness training policy; procedures addressing security literacy and awareness training records; security literacy and awareness training records; security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with security and awareness training record retention responsibilities].

Test

[SELECT FROM: Mechanisms supporting the management of security literacy and awareness training records].

REFERENCES

754 Source Assessment Procedures: AT-06

755 **03.02.04E Anti-Counterfeit Training**

756 **ASSESSMENT OBJECTIVE**

757 *Determine if:*

758 **A.03.02.04E.ODP[01]:** ***personnel or roles requiring training to detect counterfeit***
759 ***system components are defined.***

760 **A.03.02.04E:** ***<A.03.02.04E.ODP[01]: personnel or roles>*** are trained to detect
761 counterfeit system components.

762 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

763 **Examine**

764 [SELECT FROM: Supply chain risk management policy and procedures; supply chain
765 risk management plan; system and services acquisition policy; anti-counterfeit plan;
766 anti-counterfeit policy and procedures; media disposal policy; media protection
767 policy; incident response policy; training materials addressing counterfeit system
768 components; training records on the detection and prevention of counterfeit
769 components entering the system; system security plan; other relevant documents or
770 records].

771 **Interview**

772 [SELECT FROM: Personnel with information security responsibilities; personnel with
773 supply chain risk management responsibilities; personnel with responsibilities for
774 anti-counterfeit policies, procedures, and training].

775 **Test**

776 [SELECT FROM: Processes for anti-counterfeit training].

777 **REFERENCES**

778 Source Assessment Procedures: SR-11(01)

779 **3.3. Audit and Accountability**

780 **03.03.01E Audit Record Storage in Separate Environment**

781 **ASSESSMENT OBJECTIVE**

782 *Determine if:*

783 **A.03.03.01E:** audit records are stored in a repository that is part of a physically
784 different system or system component than the system or component being
785 audited.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Audit and accountability policy; system security plan; procedures addressing protection of audit information; system design documentation; system configuration settings and associated documentation; system or media storing backups of system audit records; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system/network administrators; system developers].

Test

[SELECT FROM: Mechanisms implementing the backing up of audit records].

REFERENCES

Source Assessment Procedures: AU-09(02)

03.03.02E Real-Time Alerts for Audit Processing Failures

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.02E.ODP[01]: ***real-time period requiring alerts when audit failure events (defined in A.03.03.02E.ODP[03]) occur is defined.***

A.03.03.02E.ODP[02]: ***personnel, roles, and/or locations to be alerted in real time when audit failure events (defined in A.03.03.02E.ODP[03]) occur are defined.***

A.03.03.02E.ODP[03]: ***audit logging failure events requiring real-time alerts are defined.***

A.03.03.02E: an alert is provided within ***<A.03.03.02E.ODP[01]: real-time period>*** to ***<A.03.03.02E.ODP[02]: personnel, roles, and/or locations>*** when ***<A.03.03.02E.ODP[03]: audit logging failure events>*** occur.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Audit and accountability policy; procedures addressing response to audit processing failures; system design documentation; system security plan; system configuration settings and associated documentation; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system/network administrators; system developers].

REFERENCES

Source Assessment Procedures: AU-05(02)

03.03.03E Dual Authorization for Audit Information and Actions

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.03E.ODP[01]: ***one or more of the following PARAMETER VALUES is/are selected: {movement; deletion}.***

A.03.03.03E.ODP[02]: ***audit information for which dual authorization is to be enforced is defined.***

A.03.03.03E: dual authorization is enforced for the ***<A.03.03.03E.ODP[01]: SELECTED PARAMETER VALUE(S)>*** of ***<A.03.03.03E.ODP[02]: audit information>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Audit and accountability policy; system security plan; access control policy and procedures; procedures addressing protection of audit information; system design documentation; system configuration settings and associated documentation; access authorizations; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system/network administrators].

Test

[SELECT FROM: Mechanisms implementing the enforcement of dual authorization].

REFERENCES

Source Assessment Procedures: AU-09(05)

03.03.04E Integrated Analysis of Audit Records

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.04E.ODP[01]: *one or more of the following PARAMETER VALUES is/are selected: {vulnerability scanning information; performance data; system monitoring information; <A.03.03.04E.ODP[02] data or information collected from other sources>}.*

A.03.03.04E.ODP[02]: *data or information collected from other sources to be analyzed is defined (if selected).*

A.03.03.04E: analysis of audit records is integrated with analysis of ***<A.03.03.04E.ODP[01]: SELECTED PARAMETER VALUE(S)>*** to further enhance the ability to identify inappropriate or unusual activity.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Audit and accountability policy; system security plan; procedures addressing audit review, analysis, and reporting; system design documentation; system configuration settings and associated documentation; integrated analysis of audit records, vulnerability scanning information, performance data, network monitoring information and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Personnel with audit review, analysis, and reporting responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms implementing the capability to integrate analysis of audit records with analysis of data or information sources].

REFERENCES

Source Assessment Procedures: AU-06(05)

3.4. Configuration Management

03.04.01E Withdrawn

Addressed by 03.04.08E, 03.14.04E, 03.17.03E, 03.17.04E, 03.17.05E, 03.04.01 (SP 800-171), 03.04.03 (SP 800-171), and 03.04.10 (SP 800-171).

03.04.02E Automated Unauthorized Component Detection

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.02E.ODP[01]: ***automated mechanisms used to detect the presence of unauthorized or misconfigured system components are defined.***

A.03.04.02E.ODP[02]: ***one or more of the following PARAMETER VALUES is/are selected: {disable network access by unauthorized or misconfigured system components; isolate unauthorized or misconfigured system components; notify <A.03.04.02E.ODP[03] personnel or roles>.***

A.03.04.02E.ODP[03]: ***personnel or roles to be notified when unauthorized or misconfigured system components are detected are defined (if selected).***

A.03.04.02E.a: the presence of unauthorized or misconfigured system components is detected using ***<A.03.04.02E.ODP[01]: automated mechanisms>***.

A.03.04.02E.b: one or more of the following actions is/are taken when unauthorized or misconfigured system components are detected: ***<A.03.04.02E.ODP[02]: SELECTED PARAMETER VALUE(S)>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Configuration management policy; procedures addressing system component inventory and configuration settings; configuration management plan; system configuration settings and associated documentation; system component inventory; system design documentation; change control records; common secure configuration checklists; alerts or notifications of unauthorized components within the system; system monitoring records; system maintenance records; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with component inventory and security configuration management responsibilities; personnel with responsibilities for managing automated mechanisms implementing unauthorized system component detection; personnel with information security responsibilities; system/network administrators; system developers].

Test

[SELECT FROM: Processes for the detection of unauthorized or misconfigured system components; automated processes for taking action when unauthorized or misconfigured system components are detected; automated mechanisms supporting and/or implementing the detection of unauthorized or misconfigured system components; automated mechanisms supporting and/or implementing actions taken when unauthorized or misconfigured system components are detected].

REFERENCES

Source Assessment Procedure: CM-06(01), CM-6(02), CM-08(03)

03.04.03E Automated Maintenance of System Component Inventory

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.03E.ODP[01]: ***automated mechanisms used to maintain the currency of the system component inventory are defined.***

A.03.04.03E.ODP[02]: ***automated mechanisms used to maintain the completeness of the system component inventory are defined.***

A.03.04.03E.ODP[03]: ***automated mechanisms used to maintain the accuracy of the system component inventory are defined.***

A.03.04.03E.ODP[04]: ***automated mechanisms used to maintain the availability of the system component inventory are defined.***

A.03.04.03E[01]: ***<A.03.04.03E.ODP[01]: automated mechanisms>*** are used to maintain the currency of the system component inventory.

A.03.04.03E[02]: ***<A.03.04.03E.ODP[02]: automated mechanisms>*** are used to maintain the completeness of the system component inventory.

A.03.04.03E[03]: ***<A.03.04.03E.ODP[03]: automated mechanisms>*** are used to maintain the accuracy of the system component inventory.

A.03.04.03E[04]: ***<A.03.04.03E.ODP[04]: automated mechanisms>*** are used to maintain the availability of the system component inventory.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Configuration management policy; procedures addressing system component inventory; configuration management plan; system security plan; system design documentation; system component inventory; change control records; system maintenance records; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with component inventory management responsibilities; personnel with information security responsibilities; system developers; system/network administrators].

Test

[SELECT FROM: Processes for maintaining the system component inventory;

automated mechanisms supporting and/or implementing the system component inventory].

REFERENCES

Source Assessment Procedures: CM-08(02)

03.04.04E Automation Support for Baseline Configuration

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.04E.ODP[01]: ***automated mechanisms for maintaining the baseline configuration of the system are defined.***

A.03.04.04E[01]: the currency of the baseline configuration of the system is maintained using ***<A.03.04.04E.ODP[01]: automated mechanisms>***.

A.03.04.04E[02]: the completeness of the baseline configuration of the system is maintained using ***<A.03.04.04E.ODP[01]: automated mechanisms>***.

A.03.04.04E[03]: the accuracy of the baseline configuration of the system is maintained using ***<A.03.04.04E.ODP[01]: automated mechanisms>***.

A.03.04.04E[04]: the availability of the baseline configuration of the system is maintained using ***<A.03.04.04E.ODP[01]: automated mechanisms>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; system component inventory; configuration change control records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with configuration management responsibilities; personnel with information security responsibilities; system/network administrators].

Test

[SELECT FROM: Processes for managing baseline configurations; automated mechanisms implementing baseline configuration maintenance].

REFERENCES

Source Assessment Procedures: CM-02(02)

03.04.05E Dual Authorization for System Changes

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.05E.ODP[01]: ***system components requiring dual authorization for changes are defined.***

A.03.04.05E.ODP[02]: ***system-level information requiring dual authorization for changes is defined.***

A.03.04.05E[01]: dual authorization for implementing changes to ***<A.03.04.05E.ODP[01]: system components>*** is enforced.

A.03.04.05E[02]: dual authorization for implementing changes to ***<A.03.04.05E.ODP[02]: system-level information>*** is enforced.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Configuration management policy; procedures addressing access restrictions for changes to the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system audit records; system component inventory; system information types; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with dual authorization enforcement responsibilities for implementing system changes; personnel with information security responsibilities; system/network administrators].

Test

[SELECT FROM: Processes for managing access restrictions to change; mechanisms implementing dual authorization enforcement].

REFERENCES

Source Assessment Procedures: CM-05(04)

03.04.06E Retention of Previous Configurations

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.06E.ODP[01]: *the number of previous baseline configuration versions to be retained is defined.*

A.03.04.06E: *<A.03.04.06E.ODP[01]: number>* previous versions of baseline configurations of the system are retained to support rollback.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; system architecture and configuration documentation; system configuration settings and associated documentation; copies of previous baseline configuration versions; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with configuration management responsibilities; personnel with information security responsibilities; system/network administrators].

Test

[SELECT FROM: Processes for managing baseline configurations].

REFERENCES

Source Assessment Procedures: CM-02(03)

03.04.07E Testing, Validation, and Documentation of Changes

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.07E[01]: changes to the system are tested before finalizing the implementation of the changes.

A.03.04.07E[02]: changes to the system are validated before finalizing the implementation of the changes.

A.03.04.07E[03]: changes to the system are documented before finalizing the implementation of the changes.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Configuration management policy; configuration management plan; procedures addressing system configuration change control; system architecture and configuration documentation; system design documentation; test records; system configuration settings and associated documentation; validation records;

change control records; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with configuration change control responsibilities; personnel with information security responsibilities; members of change control board or similar; system/network administrators; system developers].

Test

[SELECT FROM: Processes for configuration change control; mechanisms supporting and/or implementing, testing, validating, and documenting system changes].

REFERENCES

Source Assessment Procedures: CM-03(02)

03.04.08E Centralized Repository

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.08E: a centralized repository for the inventory of system components is provided.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Configuration management policy; procedures addressing system component inventory; configuration management plan; system design documentation; system security plan; system component inventory; system configuration settings and associated documentation; change control records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel with component inventory management responsibilities; organizational personnel with security responsibilities].

Test

[SELECT FROM: Organizational processes for managing the system component inventory; mechanisms supporting and/or implementing system component inventory].

REFERENCES

Source Assessment Procedures: CM-08(07)

3.5. Identification and Authentication

03.05.01E Cryptographic Bidirectional Authentication

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.01E.ODP[01]: ***devices and/or types of devices requiring the use of cryptographically based bidirectional authentication to authenticate before establishing a system connection are defined.***

A.03.05.01E: ***<A.03.05.01E.ODP[01]: devices and/or types of devices>*** are authenticated before establishing a system connection using bidirectional authentication that is cryptographically based.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing device identification and authentication; system design documentation; configuration settings and associated documentation; list of devices requiring unique identification and authentication; device connection reports; other relevant documents or records].

Interview

[SELECT FROM: Personnel with operational responsibilities for device identification and authentication; personnel with information security responsibilities; system/network administrators; system developers].

Test

[SELECT FROM: Mechanisms supporting and/or implementing device authentication capabilities; cryptographically based bidirectional authentication mechanisms].

REFERENCES

Source Assessment Procedures: IA-03(01)

03.05.02E Password Managers

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.02E.ODP[01]: ***password managers employed for generating and managing passwords are defined.***

A.03.05.02E: ***<A.03.05.02E.ODP[01]: password managers>*** are employed to generate and manage passwords.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Identification and authentication policy; procedures addressing identifier management; system security plan; system design documentation; mechanisms providing dynamic binding of identifiers and authenticators; system configuration settings and associated documentation; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with identification and authentication management responsibilities; personnel with information security responsibilities; system/network administrators].

Test

[SELECT FROM: Mechanisms supporting and/or implementing account management capabilities; mechanisms supporting and/or implementing identification and authentication management capabilities for the system].

REFERENCES

Source Assessment Procedures: IA-05(18)

03.05.03E Device Attestation

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.03E.ODP[01]: ***the configuration management process employed to handle device identification and authentication based on attestation is defined.***

A.03.05.03E: device identification and authentication are handled based on attestation by ***<A.03.05.02E.ODP[01]: configuration management process>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing device identification and authentication; procedures addressing device configuration management; system design documentation; system configuration settings and associated documentation; configuration management records; change control records; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with operational responsibilities for device identification and authentication; personnel with information security responsibilities; system/network administrators].

Test

[SELECT FROM: Mechanisms supporting and/or implementing device identification and authentication capabilities; mechanisms supporting and/or implementing configuration management; cryptographic mechanisms supporting device attestation].

REFERENCES

Source Assessment Procedures: IA-03(04)

03.05.04E No Embedded Unencrypted Static Authenticators

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.04E: unencrypted static authenticators are not embedded in applications or other forms of static storage.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing authenticator management; system design documentation; system configuration settings and associated documentation; logical access scripts; application code reviews for detecting unencrypted static authenticators; other relevant documents or records].

Interview

[SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system/network administrators; system developers].

Test

[SELECT FROM: Mechanisms supporting and/or implementing authenticator management capabilities; mechanisms implementing authentication in applications].

REFERENCES

Source Assessment Procedures: IA-05(07)

03.05.05E Expiration of Cached Authenticators

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.05E.ODP[01]: ***the time period after which the use of cached authenticators is prohibited is defined.***

A.03.05.05E: the use of cached authenticators is prohibited after ***<A.03.05.05E.ODP[01]: time period>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Identification and authentication policy; procedures addressing authenticator management; system security plan; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with authenticator management responsibilities; personnel with information security responsibilities; system/network administrators; system developers].

Test

[SELECT FROM: Mechanisms supporting and/or implementing authenticator management capabilities].

REFERENCES

Source Assessment Procedures: IA-05(13)

03.05.06E Identity Proofing

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.06E.a: users who require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines are identity-proofed.

A.03.05.06E.b: user identities are resolved to a unique individual.

A.03.05.06E.c[01]: identity evidence is collected.

A.03.05.06E.c[02]: identity evidence is validated.

A.03.05.06E.c[03]: identity evidence is verified.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Identification and authentication policy; procedures addressing identity proofing; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system operations responsibilities; personnel with information security responsibilities; system/network administrators; system developers; personnel with identification and authentication responsibilities].

Test

[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities].

REFERENCES

Source Assessment Procedure: IA-12

03.05.07E Identity Providers and Authorization Servers

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.07E.ODP[01]: an *identification and authentication policy is defined.*

A.03.05.07E.ODP[02]: *mechanisms supporting authentication and authorization decisions are defined.*

A.03.05.07E[01]: identity providers are employed to manage user, device, and non-person entity identities, attributes, and access rights supporting authentication decisions in accordance with ***<A.03.05.07E.ODP[01]: policy>*** using ***<A.03.05.07E.ODP[02]: mechanisms>*.**

A.03.05.07E[02]: identity providers are employed to manage user, device, and non-person entity identities, attributes, and access rights supporting authorization decisions in accordance with ***<A.03.05.07E.ODP[01]: policy>*** using ***<A.03.05.07E.ODP[02]: mechanisms>.***

A.03.05.07E[03]: authorization servers are employed to manage user, device, and non-person entity identities, attributes, and access rights supporting authentication decisions in accordance with ***<A.03.05.07E.ODP[01]: policy>*** using <***A.03.05.07E.ODP[02]: mechanisms>.***

A.03.05.07E[02]: authorization servers are employed to manage user, device, and non-person entity identities, attributes, and access rights supporting authorization decisions in accordance with ***<A.03.05.07E.ODP[01]: policy>*** using ***<A.03.05.07E.ODP[02]: mechanisms>.***

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Identification and authentication policy; procedures addressing user and device identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with account management responsibilities; system developers].

Test

[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities and access rights].

REFERENCES

Source Assessment Procedure: IA-13

3.6. Incident Response

03.06.01E Security Operations Center

ASSESSMENT OBJECTIVE

Determine if:

A.03.06.01E[01]: a security operations center is established.

A.03.06.01E[02]: a security operations center 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; mechanisms supporting dynamic response capabilities; system security plan; contingency plan; incident response plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with incident handling responsibilities; personnel with information security responsibilities; security operations center personnel; personnel with contingency planning responsibilities].

Test

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

REFERENCES

Source Assessment Procedures: IR-04(14)

03.06.02E Integrated Incident Response Team

ASSESSMENT OBJECTIVE

Determine if:

A.03.06.02E.ODP[01]: ***the time period within which an integrated incident response team can be deployed is defined.***

A.03.06.02E[01]: an integrated incident response team is established.

A.03.06.02E[02]: an integrated incident response team is maintained.

A.03.06.02E[03]: the integrated incident response team can be deployed to any location identified by the organization in ***<A.03.06.02E.ODP[01]: time period>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Incident response policy; procedures addressing incident handling; procedures addressing incident response planning; incident response plan; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with incident handling responsibilities; personnel with information security responsibilities; members of the integrated incident response team].

REFERENCES

Source Assessment Procedures: IR-04(11)

03.06.03E Behavior Analysis

ASSESSMENT OBJECTIVE

Determine if:

A.03.06.03E.ODP[01]: ***environments or resources that may contain or be related to anomalous or suspected adversarial behavior are defined.***

A.03.06.03E: anomalous or suspected adversarial behavior in or related to ***<A.03.06.03E.ODP[01]: environments or resources>*** is analyzed.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Incident response policy; procedures addressing system monitoring tools and techniques; incident response plan; system monitoring logs or records; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system security plan; system component inventory; network diagram; system protocols documentation; list of acceptable thresholds for false positives and false negatives; other relevant documents or records].

Interview

[SELECT FROM: Personnel with information security responsibilities; system/network administrators].

Test

[SELECT FROM: Processes for detecting anomalous behavior].

REFERENCES

Source Assessment Procedures: IR-04(13)

03.06.04E Automated Tracking, Data Collection, and Analysis for Incident Monitoring

ASSESSMENT OBJECTIVE

Determine if:

A.03.06.04E.ODP[01]: ***automated mechanisms used to track incidents are defined.***

A.03.06.04E.ODP[02]: ***automated mechanisms used to collect incident information are defined.***

A.03.06.04E.ODP[03]: ***automated mechanisms used to analyze incident information are defined.***

A.03.06.04E[01]: incidents are tracked using ***<A.03.06.04E.ODP[01]: automated mechanisms>***.

A.03.06.04E[02]: incident information is collected using ***<A.03.06.04E.ODP[02]: automated mechanisms>***.

A.03.06.04E[03]: incident information is analyzed using ***<A.03.06.04E.ODP[03]: automated mechanisms>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; system security plan; incident response plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with incident monitoring responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Incident monitoring capability for the organization; automated mechanisms supporting and/or implementing the tracking and documenting of system security incidents].

REFERENCES

Source Assessment Procedures: IR-05(01)

3.7. Maintenance

03.07.01E Software Updates and Patches for Maintenance Tools

ASSESSMENT OBJECTIVE

Determine if:

A.03.07.01E: maintenance tools are inspected to ensure that the latest software updates and patches are installed.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; list of personnel authorized to use maintenance tools; maintenance tool usage records; maintenance records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system maintenance responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Processes for inspecting maintenance tools; processes for maintenance tool updates; mechanisms supporting and/or implementing the inspection of maintenance tools; mechanisms supporting and/or implementing maintenance tool updates].

REFERENCES

Source Assessment Procedures: MA-03(06)

3.8. Media Protection

03.08.01E Dual Authorization for Media Sanitization

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.01E.ODP[01]: ***system media containing CUI to be sanitized requiring dual authorization is defined.***

A.03.08.01E: dual authorization for the sanitization of ***<A.03.08.01E.ODP[01]: system media>*** is enforced.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System media protection policy; procedures addressing media sanitization and disposal; dual authorization policy and procedures; list of system media requiring dual authorization for sanitization; authorization records; media sanitization records; audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system media sanitization responsibilities; personnel with information security responsibilities; system/network administrators].

Test

[SELECT FROM: Processes requiring dual authorization for media sanitization; mechanisms supporting and/or implementing media sanitization; mechanisms supporting and/or implementing dual authorization].

REFERENCES

Source Assessment Procedures: MP-06(07)

03.08.02E Dual Authorization for System Backup Deletion and Destruction

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.02E.ODP[01]: system *backup information for which to enforce dual authorization in order to delete or destroy is defined.*

A.03.08.02E: dual authorization for the deletion or destruction of ***<A.03.08.02E.ODP[01]: system backup information>*** is enforced.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; system design documentation; system configuration settings and associated documentation; system-generated list of dual authorization credentials or rules; logs or records of the deletion or destruction of backup information; system security plan; other relevant documents or records]

Interview

[SELECT FROM: Personnel with system backup responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms supporting and/or implementing dual authorization; mechanisms supporting and/or implementing the deletion and/or destruction of backup information].

REFERENCES

Source Assessment Procedures: CP-09(07)

03.08.03E Testing System Backups for Reliability and Integrity

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.03E.ODP[01]: *the frequency at which to test backup information for media reliability is defined.*

A.03.08.03E.ODP[02]: *the frequency at which to test backup information for information integrity is defined.*

A.03.08.03E[01]: backup information is tested ***<A.03.08.03E.ODP[01]: frequency>*** to verify media reliability.

A.03.08.03E[02]: backup information is tested ***<A.03.08.03E.ODP[02]: frequency>*** to

verify information integrity.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; system backup test results; contingency plan test documentation; contingency plan test results; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system backup responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Processes for conducting system backups; mechanisms supporting and/or implementing system backups].

REFERENCES

Source Assessment Procedures: CP-09(01)

03.08.04E System Recovery and Reconstitution

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.04E.ODP[01]: a *time period consistent with recovery time and recovery point objectives for the recovery of the system is determined*.

A.03.08.04E.ODP[02*]: a time period consistent with recovery time and recovery point objectives for the reconstitution of the system is determined.*

A.03.08.04E[01]: the recovery of the system to a known state is provided within ***<A.03.08.07E.ODP[01]: time period>*** after a disruption, compromise, or failure.

A.03.08.04E[02]: the reconstitution of the system to a known state is provided within ***<A.03.08.07E.ODP[02]: time period>*** after a disruption, compromise, or failure.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; system backup test results; contingency plan test results; contingency plan test documentation; redundant secondary system for system backups; locations of redundant secondary backup systems; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel with contingency planning, recovery, and/or reconstitution responsibilities; organizational personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes implementing system recovery and reconstitution operations; mechanisms supporting and/or implementing system recovery and reconstitution operations].

REFERENCES

Source Assessment Procedures: CP-10

3.9. Personnel Security

03.09.01E Withdrawn

Addressed by 03.09.01.

03.09.02E Withdrawn

Addressed by 03.01.01 and 03.09.01.

03.09.03E Access Agreements

ASSESSMENT OBJECTIVE

Determine if:

A.03.09.03E.ODP[01]: ***the frequency at which to review and update access agreements is defined.***

A.03.09.03E.ODP[02]: ***the frequency at which to re-sign access agreements to maintain access systems processing, storing, or transmitting CUI is defined.***

A.03.09.03E.a: access agreements are developed and documented for systems processing, storing, or transmitting CUI.

A.03.09.03E.b[01]: access agreements are reviewed ***<A.03.09.03E.ODP[01]: frequency>***.

A.03.09.03E.b[02]: access agreements are updated ***<A.03.09.03E.ODP[01]: frequency>***.

A.03.09.03E.c.01: individuals requiring access to CUI and systems processing, storing, or transmitting CUI sign appropriate access agreements prior to being granted access.

A.03.09.03E.c.02: individuals requiring access to CUI and systems processing, storing, or transmitting CUI re-sign access agreements to maintain access when access agreements have been updated or ***<A.03.09.03E.ODP[02]: frequency>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Personnel security policy; personnel security procedures; procedures addressing access agreements for systems processing, storing, or transmitting CUI; access control policy; access control procedures; access agreements (including non-disclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements); documentation of access agreement reviews, updates, and re-signing; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with personnel security responsibilities; personnel who have signed and/or resigned access agreements; personnel with information security responsibilities].

Test

[SELECT FROM: Processes for reviewing, updating, and re-signing access agreements; mechanisms supporting reviewing, updating, and re-signing of access agreements].

REFERENCES

Source Assessment Procedures: PS-06

03.09.04E Citizenship Requirements

ASSESSMENT OBJECTIVE

Determine if:

A.03.09.04E.ODP[01]: citizenship requirements to be met by individuals to access a system processing, storing, or transmitting CUI are defined.

A.03.09.04E: individuals accessing a system processing, storing, or transmitting CUI meet **<A.03.09.04E.ODP[01] citizenship requirements>**.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Personnel security policy; access control policy, procedures addressing personnel screening; records of screened personnel; screening criteria; records of access authorizations; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with personnel security responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Processes for ensuring valid access authorizations for accessing CUI and systems requiring citizenship; processes for additional personnel screening].

REFERENCES

Source Assessment Procedures: PS-03(04)

3.10. Physical Protection

03.10.01E Intrusion Alarms and Surveillance Equipment

ASSESSMENT OBJECTIVE

Determine if:

A.03.10.01E[01]: physical access to the facility where the system resides is monitored using physical intrusion alarms.

A.03.10.01E[02]: physical access to the facility where the system resides is monitored using physical surveillance equipment.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; physical access monitoring records; physical access log reviews; physical access logs or records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with physical access monitoring responsibilities; personnel with incident response responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Processes for monitoring physical intrusion alarms and surveillance equipment; mechanisms supporting and/or implementing physical intrusion alarms

and surveillance equipment; mechanisms supporting and/or implementing physical access monitoring].

REFERENCES

Source Assessment Procedures: PE-06(01)

03.10.02E Delivery and Removal of System Components

ASSESSMENT OBJECTIVE

Determine if:

A.03.10.02E.ODP[01]: ***the types of system components to be authorized and controlled when entering the facility are defined.***

A.03.10.02E.ODP[02]: ***the types of system components to be authorized and controlled when exiting the facility are defined.***

A.03.10.02E.a[01]: ***<A.03.10.02E.ODP[01]: types of system components>*** are authorized when entering the facility.

A.03.10.02E.a[02]: ***<A.03.10.02E.ODP[01]: types of system components>*** are controlled when entering the facility.

A.03.10.02E.a[03]: ***<A.03.10.02E.ODP[02]: types of system components>*** are authorized when exiting the facility.

A.03.10.02E.a[04]: ***<A.03.10.02E.ODP[02]: types of system components>*** are controlled when exiting the facility.

A.03.10.02E.b: records of the system components entering and exiting the facility are maintained.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Physical and environmental protection policy; procedures addressing the delivery and removal of system components from the facility; facility housing the system; records of items entering and exiting the facility; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for controlling system components entering and exiting the facility; personnel with information security responsibilities].

Test

[SELECT FROM: Process for authorizing, monitoring, and controlling system-related items entering and exiting the facility; mechanisms supporting and/or implementing,

authorizing, monitoring, and controlling system components entering and exiting the facility].

REFERENCES

Source Assessment Procedures: PE-16

3.11. Risk Assessment

03.11.01E Threat Awareness Program

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.01E: a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence is implemented.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Information security program plan; threat awareness program policy; threat awareness program procedures; risk assessment results relevant to threat awareness; documentation about the cross-organization information-sharing capability; other relevant documents or records].

Interview

[SELECT FROM: Personnel with information security program planning and plan implementation responsibilities; personnel responsible for the threat awareness program; personnel responsible for the cross-organization information-sharing capability; personnel with information security responsibilities; external personnel with whom threat awareness information is shared by the organization].

Test

[SELECT FROM: Processes for implementing the threat awareness program; processes for implementing the cross-organization information-sharing capability; mechanisms supporting and/or implementing the threat awareness program; mechanisms supporting and/or implementing the cross-organization information-sharing capability].

REFERENCES

Source Assessment Procedures: PM-16

03.11.02E Threat Hunting

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.02E.ODP[01]: *the frequency at which to employ the threat-hunting capability is defined.*

A.03.11.02E.a.01[01]: a cyber threat capability is established to search for indicators of compromise in organizational systems.

A.03.11.02E.a.01[02]: a cyber threat capability is maintained to search for indicators of compromise in organizational systems.

A.03.11.02E.a.02[01]: a cyber threat capability is established to detect, track, and disrupt threats that evade existing safeguards.

A.03.11.02E.a.02[02]: a cyber threat capability is maintained to detect, track, and disrupt threats that evade existing safeguards.

A.03.11.02E.b: the threat-hunting capability is employed***<A.03.11.02E.ODP[01]: frequency>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Risk assessment policy; assessment reports; audit records and/or event logs; threat-hunting capability; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with threat-hunting responsibilities; system/network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Processes for assessments and audits; mechanisms or tools supporting and/or implementing threat-hunting capabilities].

REFERENCES

Source Assessment Procedures: RA-10

03.11.03E Predictive Cyber Analytics

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.03E.ODP[01]: ***advanced automation capabilities to predict and identify risks are defined.***

A.03.11.03E.ODP[02]: ***systems or system components in which advanced automation and analytics capabilities are to be employed are defined.***

A.03.11.03E.ODP[03]: ***advanced analytics capabilities to predict and identify risks are defined.***

A.03.11.03E[01]: ***<A.03.11.03E.ODP[01]: advanced automation capabilities>*** are employed to predict and identify risks to ***<A.03.11.03E.ODP[02]: systems or system components>***.

A.03.11.03E[02]: ***<A.03.11.03E.ODP[03]: advanced analytics capabilities>*** are employed to predict and identify risks to ***<A.03.11.03E.ODP[02]: systems or system components>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; risk reports; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with risk assessment responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Processes for risk assessment; mechanisms supporting and/or conducting, documenting, reviewing, disseminating, and updating the risk assessment].

REFERENCES

Source Assessment Procedures: RA-03(04)

03.11.04E Withdrawn

Addressed by 03.15.01E, 03.11.01 (SP 800-171), 03.11.04 (SP 800-171), and 03.15.02 (SP 800-171).

03.11.05E Withdrawn

Addressed by 03.11.01E, 03.11.03E, 03.11.01 (SP 800-171), 03.11.04 (SP 800-171), 03.12.01 (SP 800-171), and 03.12.03 (SP 800-171).

03.11.06E Withdrawn

Addressed by 03.12.03E, 03.11.01 (SP 800-171), 03.11.04 (SP 800-171), 03.12.01 (SP 800-171), 03.12.03 (SP 800-171), and 03.17.03 (SP 800-171).

03.11.07E Withdrawn

Addressed by 03.17.01 (SP 800-171).

03.11.08E Dynamic Threat Awareness

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.08E.ODP[01]: ***the means to determine the current cyber threat environment on an ongoing basis are defined.***

A.03.11.08E: the current cyber threat environment is determined on an ongoing basis using ***<A.03.11.08E.ODP[01]: means>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; risk reports; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with risk assessment responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Processes for risk assessment; mechanisms supporting and/or conducting, documenting, reviewing, disseminating, and updating the risk assessment].

REFERENCES

Source Assessment Procedures: RA-03(03)

03.11.09E Indicators of Compromise

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.09E.ODP[01]: ***sources that provide indicators of compromise are defined.***

A.03.11.09E.ODP[02]: ***personnel or roles to whom indicators of compromise are to be distributed are defined.***

A.03.11.09E[01]: indicators of compromise provided by ***<A.03.11.09E.ODP[01]: sources>*** are discovered.

A.03.11.09E[02]: indicators of compromise provided by ***<A.03.11.09E.ODP[01]: sources>*** are collected.

A.03.11.09E[03]: indicators of compromise provided by ***<A.03.11.09E.ODP[01]: sources>*** are distributed to ***<A.03.11.09E.ODP[02]: personnel or roles>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system monitoring logs or records; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; system developers; personnel installing, configuring, and/or maintaining the system; personnel responsible for monitoring system hosts].

Test

[SELECT FROM: Processes for system monitoring; processes for the discovery, collection, distribution, and use of indicators of compromise; mechanisms supporting and/or implementing a system monitoring capability; mechanisms supporting and/or implementing the discovery, collection, distribution, and use of indicators of compromise].

REFERENCES

Source Assessment Procedures: SI-04(24)

03.11.10E Criticality Analysis

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.10E.ODP[01]: ***systems, system components, or system services to be analyzed for criticality are defined.***

A.03.11.10E.ODP[02]: ***decision points in the system development life cycle when a criticality analysis is to be performed are defined.***

A.03.11.10E: critical system components and functions are identified by performing a criticality analysis for ***<A.03.11.10E.ODP[01]: systems, system components, or system services>*** at ***<A.03.11.10E.ODP[02]: decision points>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Risk assessment policy; assessment reports; criticality analysis and/or finalized criticality for each component and/or subcomponent; audit records and/or event logs; analysis reports; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with assessment and auditing responsibilities; personnel with criticality analysis responsibilities; system/network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Processes for assessments and audits; mechanisms and/or tools supporting and/or implementing assessments and auditing].

REFERENCES

Source Assessment Procedures: RA-09

03.11.11E Discoverable Information

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.11E.ODP[01]: ***corrective actions to be taken if information about the system is discoverable are defined.***

A.03.11.11E[01]: discoverable information about the system is identified.

A.03.11.11E[02]: ***<A.03.11.11E.ODP[01]: corrective actions>*** are taken when information about the system is confirmed as discoverable.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Procedures addressing vulnerability scanning; assessment report; penetration test results; vulnerability scanning results; risk assessment report; records of corrective actions taken on discoverable information; incident response records; audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with vulnerability scanning and/or penetration testing responsibilities; personnel with vulnerability scan analysis responsibilities; personnel responsible for risk response; personnel responsible for incident management and response; personnel with information security responsibilities].

Test

[SELECT FROM: Processes for vulnerability scanning; processes for risk response; processes for incident management and response; mechanisms and/or tools supporting and/or implementing vulnerability scanning; mechanisms supporting and/or implementing risk response; mechanisms supporting and/or implementing incident management and response].

REFERENCES

Source Assessment Procedures: RA-05(04)

03.11.12E Automated Means for Sharing Threat Intelligence

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.12E: automated mechanisms are employed to maximize the effectiveness of sharing threat intelligence information.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Information security program plan; threat awareness program policy; threat awareness program procedures; risk assessment results related to threat awareness; documentation about the cross-organization information-sharing capability; other relevant documents or records].

Interview

[SELECT FROM: Personnel with information security program planning and plan implementation responsibilities; personnel responsible for the threat awareness program; personnel responsible for the cross-organization information-sharing capability; personnel with information security responsibilities; external personnel with whom threat awareness information is shared by the organization].

Test

[SELECT FROM: Processes for implementing the threat awareness program; processes for implementing the cross-organization information-sharing capability; automated mechanisms supporting and/or implementing the threat awareness program; automated mechanisms supporting and/or implementing the cross-organization information-sharing capability].

REFERENCES

Source Assessment Procedures: PM-16(01)

3.12. Security Assessment and Monitoring

03.12.01E Penetration Testing

ASSESSMENT OBJECTIVE

Determine if:

A.03.12.01E.ODP[01]: ***the frequency at which to conduct penetration testing on systems or system components is defined.***

A.03.12.01E.ODP[02]: ***systems or system components on which penetration testing is to be conducted are defined.***

A.03.12.01E: penetration testing is conducted ***<A.03.12.01E.ODP[01]: frequency>*** on ***<A.03.12.01E.ODP[02]: systems or system components>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Assessment and monitoring policy; procedures addressing penetration testing; assessment plan; system security plan; penetration test rules of engagement; penetration test report; assessment report; assessment evidence; other relevant documents or records].

Interview

[SELECT FROM: Personnel with assessment responsibilities; personnel with information security responsibilities; system/network administrators].

Test

[SELECT FROM: Mechanisms supporting penetration testing].

REFERENCES

Source Assessment Procedures: CA-08

03.12.02E Independent Assessors

ASSESSMENT OBJECTIVE

Determine if:

A.03.12.02E: independent assessors or assessment teams are used to conduct security requirement assessments.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Assessment and monitoring policy; procedures addressing assessments; previous assessment plan; previous assessment report; plan of action and milestones; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with assessment responsibilities; personnel with information security responsibilities].

REFERENCES

Source Assessment Procedures: CA-02(01)

03.12.03E Risk Monitoring

ASSESSMENT OBJECTIVE

Determine if:

A.03.12.03E[01]: risk monitoring is an integral part of the continuous monitoring strategy.

A.03.12.03E[02]: effectiveness monitoring is included in risk monitoring.

A.03.12.03E[03]: compliance monitoring is included in risk monitoring.

A.03.12.03E[04]: change monitoring is included in risk monitoring.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Assessment and monitoring policy; organizational continuous

monitoring strategy; system-level continuous monitoring strategy; procedures addressing continuous monitoring of system; assessment report; plan of action and milestones; system monitoring records; impact analyses; status reports; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with continuous monitoring responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms supporting risk monitoring].

REFERENCES

Source Assessment Procedures: CA-07(04)

03.12.04E Internal System Connections

ASSESSMENT OBJECTIVE

Determine if:

A.03.12.04E.ODP[01]: ***system components or classes of components requiring internal connections to the system are defined.***

A.03.12.04E.ODP[02]: ***conditions requiring the termination of internal connections are defined.***

A.03.12.04E.ODP[03]: ***the frequency at which to review the continued need for each internal connection is defined.***

A.03.12.04E.a: internal connections of ***<A.03.12.04E.ODP[01]: system components or classes of components>*** to the system are authorized.

A.03.12.04E.b[01]: for each internal connection, the interface characteristics are documented.

A.03.12.04E.b[02]: for each internal connection, the security requirements are documented.

A.03.12.04E.b[03]: for each internal connection, the nature of the information communicated is documented.

A.03.12.04E.c: internal system connections are terminated after ***<A.03.12.04E.ODP[02]: conditions>***.

A.03.12.04E.d: the continued need for each internal connection is reviewed ***<A.03.12.04E.ODP[03]: frequency>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Assessment and monitoring policy; access control policy; procedures addressing system connections; system and communications protection policy; system design documentation; system audit records; list of components or classes of components authorized as internal system connections; system security plan; system configuration settings and associated documentation; assessment report; other relevant documents or records].

Interview

[SELECT FROM: Personnel with responsibilities for developing, implementing, or authorizing internal system connections; personnel with information security and responsibilities].

Test

[SELECT FROM: Mechanisms supporting internal system connections].

REFERENCES

Source Assessment Procedures: CA-09

3.13. System and Communications Protection

03.13.01E Heterogeneity

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.01E.ODP[01]: ***system components requiring a diverse set of information technologies to be employed in the implementation of the system are defined.***

A.03.13.01E: a diverse set of information technologies is employed for ***<A.03.13.01E.ODP[01]: system components>*** in the implementation of the system.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; system design documentation; system configuration settings and associated documentation; list of technologies deployed in the system; acquisition documentation; acquisition contracts for system components or services; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; personnel with system acquisition, development, and implementation responsibilities].

Test

[SELECT FROM: Mechanisms supporting and/or implementing the use of a diverse set of information technologies].

REFERENCES

Source Assessment Procedures: SC-29

03.13.02E Randomness

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.02E.ODP[01]: ***the techniques employedd to introduce randomness into organizational operations and assets are defined.***

A.03.13.02E: ***<A.03.13.02E.ODP[01]: techniques>*** are employed to introduce randomness into organizational operations and assets.

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; system configuration settings and associated documentation; system architecture; list of techniques to be used to introduce randomness into organizational operations and assets; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with the responsibility to implement concealment and misdirection techniques for systems; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms supporting and/or implementing randomness as a concealment and misdirection technique].

REFERENCES

Source Assessment Procedures: SC-30(02)

03.13.03E Concealment and Misdirection

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.03E.ODP[01]: ***the concealment and misdirection techniques employed to mislead adversaries potentially targeting systems are defined.***

A.03.13.03E: ***<A.03.13.03E.ODP[01]: concealment and misdirection techniques>*** are used to mislead adversaries.

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; system configuration settings and associated documentation; system architecture; list of concealment and misdirection techniques to be used for organizational systems; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; personnel with the responsibility to implement concealment and misdirection techniques for systems].

Test

[SELECT FROM: Mechanisms supporting and/or implementing concealment and misdirection techniques].

REFERENCES

Source Assessment Procedures: SC-30

03.13.04E Isolation of System Components

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.04E.ODP[01]: ***system components to be isolated by boundary protection mechanisms are defined.***

A.03.13.04E: boundary protection mechanisms are employed to isolate ***<A.03.13.04E.ODP[01]: system components>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; enterprise architecture documentation; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; personnel with boundary protection responsibilities].

Test

[SELECT FROM: Mechanisms supporting and/or implementing the capability to separate system components].

REFERENCES

Source Assessment Procedures: SC-07(21)

03.13.05E Change Processing and Storage Locations

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.05E.ODP[01]: ***processing and/or storage locations to be changed are defined.***

A.03.13.05E.ODP[02]: ***one of the following PARAMETER VALUES is selected: {<A.03.13.05E.ODP[03] time frequency>; at random time intervals}.***

A.03.13.05E.ODP[03]: ***the time frequency at which to change the location of processing and/or storage is defined (if selected).***

A.03.13.05E: the location of ***<A.03.13.05E.ODP[01]: processing and/or storage>*** is changed ***<A.03.13.05E.ODP[02]: SELECTED PARAMETER VALUE>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; configuration management policy and procedures; procedures addressing concealment and misdirection techniques for the system; list of processing and/or storage locations to be changed at organizational time intervals; change control records; configuration management records; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; personnel with the responsibility to change processing and/or storage locations].

Test

[SELECT FROM: Mechanisms supporting and/or implementing changing processing and/or storage locations].

REFERENCES

Source Assessment Procedures: SC-30(03)

03.13.06E Platform-Independent Applications

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.06E.ODP[01]: *platform-independent applications to be included within organizational systems are defined.*

A.03.13.06E: *<A.03.13.06E.ODP[01]: platform-independent applications>* are implemented within organizational systems.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; procedures addressing platform-independent applications; system design documentation; system configuration settings and associated documentation; list of platform-independent applications; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms supporting and/or implementing platform-independent applications].

REFERENCES

Source Assessment Procedures: SC-27

03.13.07E Virtualization Techniques

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.07E.ODP[01]: ***the frequency at which to change the diversity of operating systems and applications deployed using virtualization techniques is defined.***

A.03.13.07E: virtualization techniques are employed to support the deployment of a diverse range of operating systems and applications that are changed ***<A.03.13.07E.ODP[01]: frequency>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; configuration management policy and procedures; system design documentation; system configuration settings and associated documentation; system architecture; list of operating systems and applications deployed using virtualization techniques; change control records; configuration management records; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; personnel with responsibilities for implementing approved virtualization techniques to the system].

Test

[SELECT FROM: Mechanisms supporting and/or implementing the use of a diverse set of information technologies; mechanisms supporting and/or implementing virtualization techniques].

REFERENCES

Source Assessment Procedures: SC-29(01)

03.13.08E Decoys

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.08E[01]: components within organizational systems specifically designed to be the target of malicious attacks are included to detect such attacks.

A.03.13.08E[02]: components within organizational systems specifically designed to be the target of malicious attacks are included to deflect such attacks.

A.03.13.08E[03]: components within organizational systems specifically designed to be the target of malicious attacks are included to analyze such attacks.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; procedures addressing the use of decoys; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms supporting and/or implementing decoys].

REFERENCES

Source Assessment Procedures: SC-26

03.13.09E Isolation of Security Tools, Mechanisms, and Support Components

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.09E.ODP[01]: ***information security tools, mechanisms, and support components to be isolated from other internal system components are defined.***

A.03.13.09E: ***<A.03.13.09E.ODP[01]: information security tools, mechanisms, and support components>*** are isolated from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; procedures

addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; list of security tools and support components to be isolated from other internal system components; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; personnel with boundary protection responsibilities].

Test

[SELECT FROM: Mechanisms supporting and/or implementing the isolation of information security tools, mechanisms, and support components].

REFERENCES

Source Assessment Procedures: SC-07(13)

03.13.10E Separate Subnetworks

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.10E: separate network addresses are implemented to connect to systems in different security domains.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; system developers; personnel with boundary protection responsibilities].

Test

[SELECT FROM: Mechanisms supporting and/or implementing separate network addresses or different subnets].

REFERENCES

Source Assessment Procedures: SC-07(22)

03.13.11E Thin Nodes

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.11E.ODP[01]: ***system components to be implemented with minimal functionality and information storage are defined.***

A.03.13.11E[01]: minimal functionality for ***<A.03.13.11E.ODP[01]: system components>*** is employed.

A.03.13.11E[02]: minimal information storage on ***<A.03.13.11E.ODP[01]: system components>*** is employed.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; procedures addressing use of thin nodes; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Mechanisms supporting and/or implementing thin nodes].

REFERENCES

Source Assessment Procedures: SC-25

03.13.12E Denial-of-Service Protection

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.12E.ODP[01]: ***the types of denial-of-service events to be protected against or limited are defined.***

A.03.13.12E.ODP[02]: ***one of the following PARAMETER VALUES is selected: {protected against; limited}.***

A.03.13.12E.ODP[03]: ***the safeguards to prevent the denial-of-service objective by type of denial-of-service event are defined.***

A.03.13.12E.a: the effects of ***<A.03.13.12E.ODP[01]: types of denial-of-service events>*** are ***<A.03.13.12E.ODP[02]: SELECTED PARAMETER VALUE>***.

A.03.13.12E.b: *<A.03.13.12E.ODP[03]: safeguards>* are employed to protect against or limit the effects of denial-of-service events.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; procedures addressing denial-of-service protection; list of denial-of-service attacks requiring employment of security safeguards to protect against or limit effects of such attacks; system design documentation; list of security safeguards protecting against or limiting the effects of denial-of-service attacks; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; personnel with incident response responsibilities; system developers].

Test

[SELECT FROM: Mechanisms protecting against or limiting the effects of denial-of-service attacks].

REFERENCES

Source Assessment Procedure: SC-05

03.13.13E Port and Input/Output Device Access

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.13E.ODP[01]: *connection ports or input/output devices to be disabled or removed are defined.*

A.03.13.13E.ODP[02]: *one of the following PARAMETER VALUES is selected: {physically; logically}.*

A.03.13.13E.ODP[03]: *systems or system components with connection ports or input/output devices to be disabled or removed are defined.*

A.03.13.13E: *<A.03.13.13E.ODP[01]: connection ports or input/output devices>* are ***<A.03.13.13E.ODP[02]: SELECTED PARAMETER VALUE>*** disabled or removed on ***<A.03.13.13E.ODP[03]: systems or system components>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; access control policy and procedures; procedures addressing port and input/output device access; system design documentation; system architecture; system configuration settings and associated documentation; systems or system components; list of connection ports or input/output devices to be physically disabled or removed on systems or system components; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; personnel with information security responsibilities; personnel installing, configuring, and/or maintaining the system].

Test

[SELECT FROM: Mechanisms supporting and/or implementing the disabling of connection ports or input/output devices].

REFERENCES

Source Assessment Procedure: SC-41

03.13.14E Detonation Chambers

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.14E.ODP[01]: ***the system, system component, or location in which a detonation chamber capability is to be employed is defined.***

A.03.13.14E: a detonation chamber capability is employed within the ***<A.03.13.14E.ODP[01]: system, system component, or location>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; procedures addressing detonation chambers; system configuration settings and associated documentation; system audit records; system design documentation; system security plan; other relevant documents or records].

Interview

[SELECT FROM: system/network administrators; personnel with information security responsibilities; personnel installing, configuring, and/or maintaining the system].

Test

[SELECT FROM: Mechanisms supporting and/or implementing the detonation chamber capability].

REFERENCES

Source Assessment Procedures: SC-44

03.13.15E Separate Subnets to Isolate System Components and Functions

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.15E.ODP[01]: ***one of the following PARAMETER VALUES is selected: {physically; logically}.***

A.03.13.15E.ODP[02]: ***critical system components and functions to be isolated are defined.***

A.03.13.15E: subnetworks are separated ***<A.03.13.15E.ODP[01]: SELECTED PARAMETER VALUE>*** to isolate ***<A.03.13.15E.ODP[02]: critical system components and functions>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; criticality analysis; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].

Test

[SELECT FROM: Mechanisms separating critical system components and functions].

REFERENCES

Source Assessment Procedures: SC-07(29)

03.13.16E System Partitioning

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.16E.ODP[01]: ***system components to reside in separate physical or logical domains or environments based on circumstances for the physical or logical separation of components are defined*.**

A.03.13.16E.ODP[02]: ***one of the following PARAMETER VALUES is selected: {physical; logical}.***

A.03.13.16E.ODP[03]: ***circumstances for the physical or logical separation of components are defined*.**

A.03.13.16E: the system is partitioned into ***<A.03.13.16E.ODP[01]: system components>*** residing in separate ***<A.03.13.16E.ODP[02]: SELECTED PARAMETER VALUE>*** domains or environments based on ***<A.03.13.16E.ODP[03]: circumstances>*.**

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and communications protection policy; procedures addressing system partitioning; system design documentation; system configuration settings and associated documentation; system architecture; list of system physical domains (or environments); system facility diagrams; system network diagrams; system security plan; other relevant documents or records].

Interview

[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].

Test

[SELECT FROM: Mechanisms supporting and/or implementing the physical separation of system components].

REFERENCES

Source Assessment Procedures: SC-32

3.14. System and Information Integrity

03.14.01E Software, Firmware, and Information Integrity

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.01E.ODP[01]: ***software requiring integrity verification tools to be used to detect unauthorized changes is defined.***

A.03.14.01E.ODP[02]: ***firmware requiring integrity verification tools to be used to detect unauthorized changes is defined.***

A.03.14.01E.ODP[03]: ***information requiring integrity verification tools to be used to detect unauthorized changes is defined.***

A.03.14.01E.ODP[04]: ***actions to be taken when unauthorized changes to software***

are detected are defined.

A.03.14.01E.ODP[05]: ***actions to be taken when unauthorized changes to firmware are detected are defined.***

A.03.14.01E.ODP[06]: ***actions to be taken when unauthorized changes to information are detected are defined.***

A.03.14.01E.a[01]: integrity verification tools are employed to detect unauthorized changes to ***<A.03.14.01E.ODP[01]: software>***.

A.03.14.01E.a[02]: integrity verification tools are employed to detect unauthorized changes to ***<A.03.14.01E.ODP[02]: firmware>***.

A.03.14.01E.a[03]: integrity verification tools are employed to detect unauthorized changes to ***<A.03.14.01E.ODP[03]: information>***.

A.03.14.01E.b[01]: ***<A.03.14.01E.ODP[04]: actions>*** are taken when unauthorized changes to software are detected.

A.03.14.01E.b[02]: ***<A.03.14.01E.ODP[05]: actions>*** are taken when unauthorized changes to firmware are detected.

A.03.14.01E.b[03]: ***<A.03.14.01E.ODP[06]: actions>*** are taken when unauthorized changes to information are detected.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; system configuration settings and associated documentation; integrity verification tools and associated documentation; records generated or triggered by system design documentation; integrity verification tools regarding unauthorized software, firmware, and information changes; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel responsible for software, firmware, and/or information integrity; personnel with information security responsibilities; system/network administrators].

Test

[SELECT FROM: Software, firmware, and information integrity verification tools].

REFERENCES

Source Assessment Procedure: SI-07

03.14.02E Withdrawn

Addressed by 03.14.06 (SP 800-171).

03.14.03E Withdrawn

Addressed by 03.15.01E, 03.13.16E, 03.12.01 (SP 800-171), 03.13.01 (SP 800-171), and 03.16.01 (SP 800-171).

03.14.04E Refresh From Trusted Sources

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.04E.ODP[01]: *trusted sources to obtain software and data for system component and service refreshes are defined.*

A.03.13.14E: the software and data used during system component and service refreshes are obtained from ***<A.03.14.04E.ODP[01]: trusted sources>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; system design documentation; procedures addressing non-persistence for system components; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel responsible for obtaining component and service refreshes from trusted sources; personnel with information security responsibilities].

Test

[SELECT FROM: Processes for defining and obtaining component and service refreshes from trusted sources; automated mechanisms supporting and/or implementing component and service refreshes].

REFERENCES

Source Assessment Procedures: SI-14(01)

03.14.05E Non-Persistent Information

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.05E.ODP[01]: ***one of the following PARAMETER VALUES is selected: {refresh <A.03.14.05E.ODP[02] information> <A.03.14.05E.ODP[03] frequency>; generate <A.03.14.05E.ODP[04] information> on demand}.***

A.03.14.05E.ODP[02]: ***the information to be refreshed is defined (if selected).***

A.03.14.05E.ODP[03]: ***the frequency at which to refresh information is defined (if selected).***

A.03.14.05E.ODP[04]: ***the information to be generated on demand is defined (if selected).***

A.03.14.05E.a: ***<A.03.14.05E.ODP[01]: SELECTED PARAMETER VALUE>*** is performed.

A.03.14.05E.b: information is deleted when no longer needed.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; system security plan; procedures addressing non-persistence for system components; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Personnel responsible for ensuring that information is and remains non-persistent; personnel with information security responsibilities].

Test

[SELECT FROM: Processes for ensuring that information is and remains non-persistent; automated mechanisms supporting and/or implementing component and service refreshes].

REFERENCES

Source Assessment Procedure: SI-14(02)

03.14.06E Withdrawn

Addressed by 03.11.02E and 03.11.09E.

03.14.07E Withdrawn

Addressed by 03.14.08E, 03.14.10E, 03.14.14E, , 03.17.03E, and 03.16.01 (SP 800-171).

03.14.08E Integrity Checks

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.08E.ODP[01]: ***software on which an integrity check is to be performed is defined.***

A.03.14.08E.ODP[02]: ***one or more of the following PARAMETER VALUES is/are selected: {at startup; at <A.03.14.08E.ODP[03] transitional states or security-relevant events>; <A.03.14.08E.ODP[04] frequency>}.***

A.03.14.08E.ODP[03]: ***transitional states or security-relevant events requiring integrity checks (on software) are defined (if selected).***

A.03.14.08E.ODP[04]: ***the frequency at which to perform an integrity check (on software) is defined (if selected).***

A.03.14.08E.ODP[05]: ***firmware on which an integrity check is to be performed is defined.***

A.03.14.08E.ODP[06]: ***one or more of the following PARAMETER VALUES is/are selected: {at startup; at <A.03.14.08E.ODP[07] transitional states or security-relevant events>; <A.03.14.08E.ODP[08] frequency>}.***

A.03.14.08E.ODP[07]: ***transitional states or security-relevant events requiring integrity checks (on firmware) are defined (if selected).***

A.03.14.08E.ODP[08]: ***the frequency at which to perform an integrity check (on firmware) is defined (if selected).***

A.03.14.08E.ODP[09]: ***information on which an integrity check is to be performed is defined.***

A.03.14.08E.ODP[10]: ***one or more of the following PARAMETER VALUES is/are selected: {at startup; at <A.03.14.08E.ODP[11] transitional states or security-relevant events>; <A.03.14.08E.ODP[12] frequency>}.***

A.03.14.08E.ODP[11]: ***transitional states or security-relevant events requiring integrity checks (of information) are defined (if selected).***

A.03.14.08E.ODP[12]: ***the frequency at which to perform an integrity check (of information) is defined (if selected).***

A.03.14.08E[01]: an integrity check of ***<A.03.14.08E.ODP[01]: software>*** is performed ***<A.03.14.05E.ODP[02]: SELECTED PARAMETER VALUE(S)>***.

A.03.14.08E[02]: an integrity check of ***<A.03.14.08E.ODP[05]: firmware>*** is performed ***<A.03.14.08E.ODP[06]: SELECTED PARAMETER VALUE(S)>***.

A.03.14.08E[03]: an integrity check of ***<A.03.14.08E.ODP[09]: information>*** is performed ***<A.03.14.08E.ODP[10]: SELECTED PARAMETER VALUE(S)>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity testing; system design documentation; system configuration settings and associated documentation; system security plan; integrity verification tools and associated documentation; records of integrity scans; other relevant documents or records].

Interview

[SELECT FROM: Personnel responsible for software, firmware, and/or information integrity; personnel with information security responsibilities; system/network administrators; system developers].

Test

[SELECT FROM: Software, firmware, and information integrity verification tools].

REFERENCES

Source Assessment Procedure: SI-07(01)

03.14.09E Cryptographic Protection

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.09E[01]: cryptographic mechanisms are implemented to detect unauthorized changes to software.

A.03.14.09E[02]: cryptographic mechanisms are implemented to detect unauthorized changes to firmware.

A.03.14.09E[03]: cryptographic mechanisms are implemented to detect unauthorized changes to information.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; system design documentation; system configuration settings and

associated documentation; system audit records; system security plan; cryptographic mechanisms and associated documentation; records of detected unauthorized changes to software, firmware, and information; other relevant documents or records].

Interview

[SELECT FROM: Personnel responsible for software, firmware, and/or information integrity; personnel with information security responsibilities; system/network administrators; system developers].

Test

[SELECT FROM: Software, firmware, and information integrity verification tools; cryptographic mechanisms implementing software, firmware, and information integrity].

REFERENCES

Source Assessment Procedures: SI-07(06)

03.14.10E Protection of Boot Firmware

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.10E.ODP[01]: ***mechanisms to be implemented to protect the integrity of boot firmware in system components are defined.***

A.03.14.10E.ODP[02]: ***system components requiring mechanisms to protect the integrity of boot firmware are defined.***

A.03.14.10E: ***<A.03.14.10E.ODP[01]: mechanisms>*** are implemented to protect the integrity of boot firmware in ***<A.03.14.10E.ODP[02]: system components>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; system design documentation; system configuration settings and associated documentation; system security plan; integrity verification tools and associated documentation; records of integrity verification scans; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Personnel responsible for software, firmware, and/or information integrity; personnel with information security responsibilities; system/network administrators; system developer].

Test

[SELECT FROM: Software, firmware, and information integrity verification tools; mechanisms supporting and/or implementing protection of the integrity of boot firmware; safeguards implementing protection of the integrity of boot firmware].

REFERENCES

Source Assessment Procedures: SI-07(10)

03.14.11E Integration of Detection and Response

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.11E.ODP[01]: ***security-relevant changes to the system are defined.***

A.03.14.11E: the detection of ***<A.03.14.11E.ODP[01]: changes>*** are incorporated into the organizational incident response capability.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; procedures addressing incident response; system design documentation; system configuration settings and associated documentation; incident response records; audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel responsible for software, firmware, and/or information integrity; personnel with information security responsibilities; personnel with incident response responsibilities].

Test

[SELECT FROM: Processes for incorporating the detection of unauthorized security-relevant changes into the incident response capability; mechanisms supporting and/or implementing the incorporation of detection of unauthorized security-relevant changes into the incident response capability; software, firmware, and information integrity verification tools].

REFERENCES

Source Assessment Procedures: SI-07(07)

03.14.12E Information Input Validation

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.12E.ODP[01]: *information inputs to the system requiring validity checks are defined.*

A.03.14.12E: the validity of the ***<A.03.14.12E.ODP[01]: information inputs>*** is checked.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; access control policy and procedures; separation of duties policy and procedures; procedures addressing information input validation; documentation for automated tools and applications to verify the validity of information; list of information inputs requiring validity checks; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel responsible for information input validation; personnel with information security responsibilities; system/network administrators; system developers].

Test

[SELECT FROM: Mechanisms supporting and/or implementing validity checks on information inputs].

REFERENCES

Source Assessment Procedures: SI-10

03.14.13E Error Handling

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.13E.ODP[01]: *personnel or roles to whom error messages are to be revealed are defined.*

A.03.14.13E.a: error messages that provide the information necessary for corrective actions are generated without revealing information that could be exploited.

A.03.14.13E.b: error messages are revealed only to ***<A.03.14.13E.ODP[01]: personnel or roles>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system error handling; system design documentation; system configuration settings and associated documentation; documentation providing the structure and content of error messages; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel responsible for information input validation; personnel with information security responsibilities; system/network administrators; system developers].

Test

[SELECT FROM: Processes for error handling; automated mechanisms supporting and/or implementing error handling; automated mechanisms supporting and/or implementing the management of error messages].

REFERENCES

Source Assessment Procedure: SI-11

03.14.14E Memory Protection

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.14E.ODP[01]: *safeguards to be implemented to protect the system memory from unauthorized code execution are defined.*

A.03.14.14E: *<A.03.14.14E.ODP[01]: safeguards>* are implemented to protect the system memory from unauthorized code execution.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing memory protection for the system; system design documentation; system configuration settings and associated documentation; list of security safeguards protecting system memory from unauthorized code execution; system audit records; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel responsible for memory protection; personnel with information security responsibilities; system/network administrators; system developers].

Test

[SELECT FROM: Automated mechanisms supporting and/or implementing safeguards to protect the system memory from unauthorized code execution].

REFERENCES

Source Assessment Procedure: SI-16

03.14.15E Non-Persistent System Components and Services

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.15E.ODP[01]: ***non-persistent system components and services to be implemented are defined.***

A.03.14.15E.ODP[02]: ***one or more of the following PARAMETER VALUES is/are selected: {upon end of session of use; <A.03.14.15E.ODP[03] frequency>}.***

A.03.14.15E.ODP[03]: ***the frequency at which to terminate non-persistent components and services that are initiated in a known state is defined (if selected).***

A.03.14.15E.a: ***<A.03.14.15E.ODP[01]: non-persistent system components and services>*** that are initiated in a known state are implemented.

A.03.14.15E.b: ***<A.03.14.15E.ODP[01]: non-persistent system components and services>*** that are initiated from a known state are implemented.

A.03.14.15E.c: ***<A.03.14.13E.ODP[01]: non-persistent system components and services>*** are terminated ***<A.03.14.15E.ODP[02]: SELECTED PARAMETER VALUE(S)>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; system design documentation; procedures addressing non-persistence for system components; system security plan; system configuration settings and associated documentation; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Personnel responsible for non-persistence; personnel with information security responsibilities; system/network administrators; system

developers].

Test

[SELECT FROM: Automated mechanisms supporting and/or implementing the initiation and termination of non-persistent components].

REFERENCES

Source Assessment Procedure: SI-14

03.14.16E Tainting

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.16E.ODP[01]: *systems or system components with data or capabilities to be embedded are defined.*

A.03.14.16E: data or capabilities are embedded in ***<A.03.14.16E.ODP[01]: systems or system components>*** to determine if CUI has been exfiltrated or improperly removed from the organization.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software and information integrity; system design documentation; system configuration settings and associated documentation; policy and procedures addressing the systems security engineering technique of deception; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel responsible for detecting tainted data; personnel with systems security engineering responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Automated mechanisms for post-breach detection; decoys, traps, lures, and methods for deceiving adversaries; detection and notification mechanisms].

REFERENCES

Source Assessment Procedure: SI-20

03.14.17E System-Generated Alerts

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.17E.ODP[01]: *personnel or roles to be alerted when indications of compromise are defined.*

A.03.14.17E.ODP[02]: *compromise indicators are defined.*

A.03.14.17E: *<A.03.14.17E.ODP[01]: personnel or roles>* are alerted when system-generated ***<A.03.14.17E.ODP[02]: indicators of compromise>*** occur.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; system security plan; system audit records; procedures addressing system monitoring tools and techniques; system monitoring tools and techniques documentation; list of personnel selected to receive alerts; system configuration settings and associated documentation; documentation of alerts generated based on compromise indicators; other relevant documents or records].

Interview

[SELECT FROM: Personnel with information security responsibilities; system developers; personnel installing, configuring, and/or maintaining the system; personnel responsible for monitoring the system; personnel on the system alert notification list; personnel responsible for the intrusion detection system; system/network administrators].

Test

[SELECT FROM: Processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing alerts for compromise indicators].

REFERENCES

Source Assessment Procedure: SI-04(05)

03.14.18E Automated Organization-Generated Alerts

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.18E.ODP[01]: ***personnel or roles to be alerted when indications of inappropriate or unusual activities with security implications occur are defined.***

A.03.14.18E.ODP[02]: ***automated mechanisms used to alert personnel or roles are defined.***

A.03.14.18E.ODP[03]: ***activities that trigger alerts to personnel or roles are defined.***

A.03.14.18E: ***<A.03.14.18E.ODP[01]: personnel or roles>*** are alerted using ***<A.03.14.18E.ODP[02]: automated mechanisms>*** when ***<A.03.14.18E.ODP[03]: activities>*** indicate inappropriate or unusual activities with security implications.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and information integrity policy; system and information integrity procedures; system security plan; list of inappropriate or unusual activities with security implications that trigger alerts; suspicious activity reports; system monitoring tools and techniques documentation; system design documentation; procedures addressing system monitoring tools and techniques; alerts provided to security personnel; system configuration settings and associated documentation; system monitoring logs or records; system audit records; other relevant documents or records].

Interview

[SELECT FROM: Personnel with information security responsibilities; system developers; personnel installing, configuring, and/or maintaining the system; personnel responsible for monitoring the system; personnel responsible for the intrusion detection system; system/network administrators].

Test

[SELECT FROM: Processes for intrusion detection and system monitoring; automated mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; automated mechanisms supporting and/or implementing automated alerts to security personnel].

REFERENCES

Source Assessment Procedure: SI-04(12)

3.15. Planning

03.15.01E Security Architecture

ASSESSMENT OBJECTIVE

Determine if:

A.03.15.01E.ODP[01]: ***the frequency for reviewing and updating the security architecture to reflect changes in the enterprise architecture is defined.***

A.03.15.01E.a.01: a security architecture for the system that describes the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of CUI is developed.

A.03.15.01E.a.02: a security architecture for the system that describes how the security architecture is integrated into and supports the enterprise architecture is developed.

A.03.15.01E.a.03: a security architecture for the system that describes any assumptions about and dependencies on external systems and services is developed.

A.03.15.01E.b: the security architecture is reviewed and updated ***<A.03.15.01E.ODP[01]: frequency>*** to reflect changes in the enterprise architecture.

A.03.15.01E.c: planned security architecture changes are reflected in system security plans, concept of operations, criticality analyses, organizational procedures, procurements, and acquisitions.

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; system security plan; security CONOPS for the system; records of information security architecture reviews and updates; other relevant documents or records].

Interview

[SELECT FROM: Personnel with security planning and plan implementation responsibilities; personnel with information security responsibilities; personnel with information security architecture development responsibilities].

Test

[SELECT FROM: Mechanisms supporting and/or implementing the development, review, and update of the information security architecture; processes for developing, reviewing, and updating the information security architecture].

REFERENCES

Source Assessment Procedures: PL-08

03.15.02E Defense In Depth

ASSESSMENT OBJECTIVE

Determine if:

A.03.15.02E.ODP[01]: ***security requirements to be allocated to architectural layers and locations are defined.***

A.03.15.02E.ODP[02]: ***architectural layers and locations are defined.***

A.03.15.02E.a: the security architecture for the system is designed using a defense-in-depth approach.

A.03.15.02E.b: ***<A.03.15.02E.ODP[01]: security requirements>*** are allocated to ***<A.03.15.02E.ODP[02]: architectural layers and locations>***.

A.03.15.02E.c: the security requirements allocated to the architectural layers and locations are coordinated and mutually reinforcing.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Security planning policy; procedures addressing information security architecture development; enterprise architecture documentation; information security architecture documentation; system security plan; security CONOPS for the system; other relevant documents or records].

Interview

[SELECT FROM: Personnel with information security responsibilities; personnel with information security architecture development responsibilities; personnel with security planning and plan implementation responsibilities].

Test

[SELECT FROM: Processes for designing the information security architecture; mechanisms supporting and/or implementing the design of the information security architecture].

REFERENCES

Source Assessment Procedures: PL-08(01)

03.15.03E Supplier Diversity

ASSESSMENT OBJECTIVE

Determine if:

A.03.15.03E.ODP[01]: ***safeguards to be allocated to architectural layers and locations are defined.***

A.03.15.03E.ODP[02]: ***architectural layers and locations are defined.***

A.03.15.03E: ***<A.03.15.03E.ODP[01]: safeguards>*** that are allocated to ***<A.03.15.03E.ODP[02]: architectural layers and locations>*** are obtained from different suppliers.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Security planning policy; procedures addressing information security architecture development; enterprise architecture documentation; information security architecture documentation; system security plan; security CONOPS for the system; IT acquisitions policy; other relevant documents or records].

Interview

[SELECT FROM: Personnel with acquisition responsibilities personnel with information security responsibilities; personnel with security planning and plan implementation responsibilities; personnel with information security architecture development responsibilities].

Test

[SELECT FROM: Processes for obtaining information security safeguards from different suppliers].

REFERENCES

Source Assessment Procedures: PL-08(02)

3.16. System and Services Acquisition

03.16.01E Specialization

ASSESSMENT OBJECTIVE

Determine if:

A.03.16.01E.ODP[01]: ***one or more of the following PARAMETER VALUES is/are selected: {design; modification; augmentation; reconfiguration}.***

A.03.16.01E.ODP[02]: ***systems or system components supporting mission-essential services or functions are defined.***

A.03.16.01E: ***<A.03.16.01E.ODP[01]: SELECTED PARAMETER VALUE(S)>*** is/are employed to ***<A.03.16.01E.ODP[02]: systems or system components>*** supporting mission-essential services or functions to increase the trustworthiness in those systems or components.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: System and services acquisition policy; procedures addressing design modification, augmentation, or reconfiguration of systems or system components; documented evidence of design modification, augmentation, or reconfiguration; system security plan; supply chain risk management plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system and service acquisition responsibilities; personnel with information security responsibilities; personnel with security architecture responsibilities; personnel with configuration management responsibilities].

Test

[SELECT FROM: Processes for the modification, design, augmentation, or reconfiguration of systems or system components; mechanisms supporting and/or implementing design modification, augmentation, or reconfiguration of systems or system components].

REFERENCES

Source Assessment Procedure: SA-23

3.17. Supply Chain Risk Management

03.17.01E Notification Agreements

ASSESSMENT OBJECTIVE

Determine if:

A.03.17.01E.ODP[01]: ***one or more of the following PARAMETER VALUES is/are selected: {notification of supply chain compromises; results of assessments or audits; provision of <A.03.17.01E.ODP[02]: information>}.***

A.03.17.01E.ODP[02]: ***information for which agreements and procedures are to be established is defined (if selected).***

A.03.17.01E: agreements and procedures are established with entities involved in the supply chain for the system, system components, or system service for ***<A.03.17.01E.ODP[01]: SELECTED PARAMETER VALUE(S)>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; acquisition contracts for the system, system component, or system service; procedures addressing supply chain protection; acquisition documentation; service-level agreements; system security plan; inter-organizational agreements and procedures; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system and service acquisition responsibilities; personnel with information security responsibilities; personnel with supply chain risk management responsibilities].

Test

[SELECT FROM: Processes for establishing inter-organizational agreements and procedures with supply chain entities].

REFERENCES

Source Assessment Procedure: SR-08

03.17.02E Inspection of Systems or Components

ASSESSMENT OBJECTIVE

Determine if:

A.03.17.02E.ODP[01]: ***systems or system components that require inspection are defined.***

A.03.17.02E.ODP[02]: ***one or more of the following PARAMETER VALUES is/are selected: {at random; <A.03.17.02E.ODP[03]: frequency>; upon <A.03.17.02E.ODP[04]: indications of the need for inspection>}.***

A.03.17.02E.ODP[03]: ***the frequency at which to inspect systems or system components is defined (if selected).***

A.03.17.02E.ODP[04]: ***indications of the need for an inspection of systems or system components are defined (if selected).***

A.03.17.02E: ***<A.03.17.02E.ODP[01]: systems or system components>*** are inspected ***<A.03.17.02E.ODP[02]: SELECTED PARAMETER VALUE(S)>*** to detect tampering.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; records of random inspections; inspection reports or results; assessment reports or results; acquisition documentation; acquisition contracts for the system, system component, or system service; inter-organizational agreements and procedures; system security plan; service-level agreements; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system and services acquisition responsibilities; personnel with information security responsibilities; personnel with supply chain risk management responsibilities].

Test

[SELECT FROM: Processes for establishing inter-organizational agreements and procedures with supply chain entities; processes to inspect for tampering].

REFERENCES

Source Assessment Procedure: SR-10

03.17.03E Component Authenticity

ASSESSMENT OBJECTIVE

Determine if:

A.03.17.03E.ODP[01]: ***one or more of the following PARAMETER VALUES is/are selected: {source of counterfeit component; <A.03.17.03E.ODP[02]: external reporting organizations>; <A.03.17.03E.ODP[03]: personnel or roles>}.***

A.03.17.03E.ODP[02]: ***external reporting organizations to whom counterfeit system components are to be reported are defined (if selected).***

A.03.17.03E.ODP[03]: ***personnel or roles to whom counterfeit system components are to be reported are defined (if selected).***

A.03.17.03E.a[01]: an anti-counterfeit policy is developed and implemented.

A.03.17.03E.a[02]: anti-counterfeit procedures are developed and implemented.

A.03.17.03E.a[03]: the anti-counterfeit policy and procedures include the means to detect counterfeit components entering the system.

A.03.17.03E.a[04]: the anti-counterfeit policy and procedures include the means to prevent counterfeit components from entering the system.

A.03.17.03E.b: counterfeit system components are reported to ***<A.03.17.03E.ODP[01]: SELECTED PARAMETER VALUE(S)>***.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; anti-counterfeit plan; anti-counterfeit policy and procedures; media disposal policy; media protection policy; incident response policy; reports notifying developers, manufacturers, vendors, contractors, and/or external reporting organizations of counterfeit system components; acquisition documentation; service-level agreements; acquisition contracts for the system, system component, or system service; inter-organizational agreements and procedures; records of reported counterfeit system components; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system and service acquisition responsibilities; personnel with information security responsibilities; personnel with supply chain risk management responsibilities; personnel with responsibilities for anti-counterfeit policies, procedures, and reporting].

Test

[SELECT FROM: Processes for counterfeit prevention, detection, and reporting; mechanisms supporting and/or implementing anti-counterfeit detection, prevention, and reporting].

REFERENCES

Source Assessment Procedure: SR-11

03.17.04E Provenance

ASSESSMENT OBJECTIVE

Determine if:

A.03.17.04E.ODP[01]: ***systems, system components, and associated CUI that require valid provenance are defined.***

A.03.17.04E[01]: valid provenance is documented *for* ***<A.03.17.04E.ODP[01]: systems, system components, and associated CUI>.***

A.03.17.04E[02]: valid provenance is monitored for ***<A.03.17.04E.ODP[01]: systems, system components, and associated CUI>.***

A.03.17.04E[03]: valid provenance is maintained for ***<A.03.17.04E.ODP[01]: systems, system components, and associated CUI>.***

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Supply chain risk management policy; supply chain risk management procedures; supply chain risk management plan; documentation of critical systems, critical system components, and associated data; documentation showing the history of ownership, custody, and location of and changes to critical systems or critical system components; system architecture; inter-organizational agreements and procedures; contracts; system security plan; other relevant documents or records].

Interview

[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].

Test

[SELECT FROM: Organizational processes for identifying the provenance of critical systems and critical system components; mechanisms used to document, monitor, or maintain provenance].

REFERENCES

Source Assessment Procedure: SR-04

03.17.05E Supply Chain Integrity – Pedigree

ASSESSMENT OBJECTIVE

Determine if:

A.03.17.05E.ODP[01]: ***safeguards employed to ensure the integrity of the system and system component are defined*.**

A.03.17.05E.ODP[02]: ***an analysis method to be conducted to validate the internal composition and provenance of critical or mission-essential technologies, products, and services to ensure the integrity of the system and system component is defined****.*

A.03.17.05E[01]: ***<A.03.17.05E.ODP[01]: safeguards>*** are employed to ensure the integrity of the system and system components.

A.03.17.05E[02]: ***<A.03.17.05E.ODP[02]: analysis method>*** is conducted to ensure the integrity of the system and system components.

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; procedures addressing supply chain protection; bill of materials for critical systems or system components; acquisition documentation; software identification tags; manufacturer declarations of platform attributes (e.g., serial numbers, hardware component inventory) and measurements (e.g., firmware hashes) that are tightly bound to the hardware itself; system security plan; other relevant documents or records].

Interview

[[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].

Test

[SELECT FROM: Organizational processes for identifying pedigree information; organizational processes to determine and validate the integrity of the internal composition of critical systems and critical system components; mechanisms to determine and validate the integrity of the internal composition of critical systems and critical system components].

REFERENCES

Source Assessment Procedure: SR-04(04)

References

[1] Federal Information Security Modernization Act (P.L. 113-283), December 2014. Available at https://www.govinfo.gov/app/details/PLAW-113publ283

[2] Office of Management and Budget Memorandum Circular A-130, Managing Information as a Strategic Resource, July 2016. Available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

[3] Ross RS, Pillitteri VY (2024) Enhanced Security Requirements for Protecting Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-172r3 ipd. https://doi.org/10.6028/NIST.SP.800-172r3.ipd

[4] 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) NIST SP 800-39. https://doi.org/10.6028/NIST.SP.800-39

[5] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53Ar5. https://doi.org/10.6028/NIST.SP.800-53Ar5

[6] International Organization for Standardization/International Electrotechnical Commission 15408-3:2017, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements, April 2017. Available at https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

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

[8] Committee on National Security Systems (2022) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[9] Executive Order 13556 (2010) Controlled Unclassified Information. (The White House, 2340 Washington, DC), DCPD-201000942, November 4, 2010. Available at https://www.govinfo.gov/app/details/DCPD-201000942

Appendix A. Acronyms

CNSS
Committee on National Security Systems

CUI
Controlled Unclassified Information

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Modernization Act

FOIA
Freedom of Information Act

ITL
Information Technology Laboratory

GRC
Governance, Risk, and Compliance

NIST
National Institute of Standards and Technology

ODP
Organization-Defined Parameter

OMB
Office of Management and Budget

OSCAL
Open Security Controls Assessment Language

Appendix B. Glossary

Appendix B provides definitions for the terminology used in SP 800-172A. The definitions are consistent with the definitions contained in the Committee on National Security Systems (CNSS) Glossary [8] unless otherwise noted.

agency
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. [2]

assessment
See *security control assessment*.

assessor
See *security control assessor*.

controlled unclassified information
Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. [9]

information
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. [2]

information system
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [2]

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.

risk
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. [2]

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. [8]

security assessment
See *security control assessment*.

security control
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. [2]

security control assessment
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. [2]

system
See *information system*.

system security plan
A document that describes how an organization meets or plans to meet the security requirements for a system. In particular, the system security plan describes the system boundary, the environment in which the system operates, how the security requirements are satisfied, and the relationships with or connections to other systems.

Appendix C. Summary of Enhanced Security Requirements

Table 2 provides a consolidated list of the enhanced security requirements in SP 800-172 [3].

Table 2. Enhanced security requirements

REQUIREMENT NUMBER	ENHANCED SECURITY REQUIREMENT
Access Control	
03.01.01E	Dual Authorization
03.01.02E	Non-Organizationally Owned Systems Restricted Use
03.01.03E	**Withdrawn**
03.01.04E	Concurrent Session Control
03.01.05E	Remote Access Monitoring and Control
03.01.06E	Protection of Remote Access Mechanism Information
03.01.07E	Automated Audit Actions for Account Management
03.01.08E	Account Monitoring for Atypical Usage
03.01.09E	Attribute-Based Access Control
03.01.10E	Object Security Attributes
03.01.11E	Role-Based Access Control
03.01.12E	Physical or Logical Separation of CUI Flows
03.01.13E	Metadata
03.01.14E	Security Policy Filters
03.01.15E	Data Type Identifiers
03.01.16E	Decomposition Into Policy-Relevant Subcomponents
03.01.17E	Detection of Unsanctioned Information
Awareness and Training	
03.02.01E	Advanced Literacy and Awareness Training
03.02.02E	Literacy and Awareness Training Practical Exercises
03.02.03E	Literacy and Awareness Training Feedback
03.02.04E	Anti-Counterfeit Training
Audit and Accountability	
03.03.01E	Protection of Audit Record Storage in Separate Physical Systems or Components
03.03.02E	Real-Time Alerts for Audit Processing Failures
03.03.03E	Dual Authorization for Audit Information and Actions
03.03.04E	Integrated Analysis of Audit Records
Configuration Management	
03.04.01E	**Withdrawn**
03.04.02E	Automated Unauthorized Component Detection
03.04.03E	Automation Maintenance for System Component Inventory
03.04.04E	Automation Support for Baseline Configuration
03.04.05E	Dual Authorization for System Changes
03.04.06E	Retention of Previous Configurations
03.04.07E	Testing, Validation, and Documentation of Changes
03.04.08E	Centralized Repository

REQUIREMENT NUMBER	ENHANCED SECURITY REQUIREMENT
Identification and Authentication	
03.05.01E	Cryptographic Bidirectional Authentication
03.05.02E	Password Managers
03.05.03E	Device Attestation
03.05.04E	No Embedded Unencrypted Static Authenticators
03.05.05E	Expiration of Cached Authenticators
03.05.06E	Identity Proofing
03.05.07E	Identity Providers and Authentication Servers
Incident Response	
03.06.01E	Security Operations Center
03.06.02E	Integrated Incident Response Team
03.06.03E	Behavior Analysis
03.06.04E	Automated Tracking, Data Collection, and Analysis for Incident Reporting
Maintenance	
03.07.01E	Software Updates and Patches for Maintenance Tools
Media Protection	
03.08.01E	Dual Authorization for Media Sanitization
03.08.02E	Dual Authorization for System Backup Deletion and Destruction
03.08.03E	Testing System Backups for Reliability and Integrity
03.08.04E	System Recovery and Reconstitution
Personnel Security	
03.09.01E	**Withdrawn**
03.09.02E	**Withdrawn**
03.09.03E	Access Agreements
03.09.04E	Citizenship Requirements
Physical Protection	
03.10.01E	Intrusion Alarms and Surveillance Equipment
03.10.02E	Delivery and Removal of System Components
Risk Assessment	
03.11.01E	Threat Awareness Program
03.11.02E	Threat Hunting
03.11.03E	Predictive Cyber Analytics
03.11.04E	**Withdrawn**
03.11.05E	**Withdrawn**
03.11.06E	**Withdrawn**
03.11.07E	**Withdrawn**
03.11.08E	Dynamic Threat Awareness
03.11.09E	Indicators of Compromise
03.11.10E	Criticality Analysis
03.11.11E	Discoverable Information
03.11.12E	Automated Means for Sharing Threat Intelligence

REQUIREMENT NUMBER	ENHANCED SECURITY REQUIREMENT
Security Assessment and Monitoring	
03.12.01E	Penetration Testing
03.12.02E	Independent Assessors
03.12.03E	Risk Monitoring
03.12.04E	Internal System Connections
System and Communications Protection	
03.13.01E	Heterogeneity
03.13.02E	Randomness
03.13.03E	Concealment and Misdirection
03.13.04E	Isolation of System Components
03.13.05E	Change Processing and Storage Locations
03.13.06E	Platform-Independent Applications
03.13.07E	Virtualization Techniques
03.13.08E	Decoys
03.13.09E	Isolation of Security Tool, Mechanism, and Support Components Isolation
03.13.10E	Separate Subnetworks
03.13.11E	Thin Nodes
03.13.12E	Denial-of-Service Protection
03.13.13E	Port and Input/Output Device Access
03.13.14E	Detonation Chambers
03.14.15E	Separate Subnets to Isolate System Components and Functions
03.14.16E	System Partitioning
System and Information Integrity	
03.14.01E	Software, Firmware, and Information Integrity
03.14.02E	**Withdrawn**
03.14.03E	**Withdrawn**
03.14.04E	Refresh from Trusted Sources
03.14.05E	Non-Persistent Information
03.14.06E	**Withdrawn**
03.14.07E	**Withdrawn**
03.14.08E	Integrity Checks
03.14.09E	Cryptographic Protection
03.14.10E	Protection of Boot Firmware
03.14.11E	Integration of Detection and Response
03.14.12E	Information Input Validation
03.14.13E	Error Handling
03.14.14E	Memory Protection
03.14.15E	Non-Persistent System Components and Services
03.14.16E	Tainting
03.14.17E	System-Generated Alerts
03.14.18E	Automated Organization-Generated Alerts
Planning	

REQUIREMENT NUMBER	ENHANCED SECURITY REQUIREMENT
03.15.01E	Security Architecture
03.15.02E	Defense In Depth
03.15.03E	Supplier Diversity
System and Services Acquisition	
03.16.01E	Specialization
Supply Chain Risk Management	
03.17.01E	Notification Agreements
03.17.02E	Inspection of Systems or Components
03.17.03E	Component Authenticity
03.17.04E	Provenance
03.17.05E	Supply Chain Integrity – Pedigree

3149

Appendix D. Security Requirement Assessments

This appendix provides an overview of the process for assessing the security requirements in SP 800-172 [3]. The four-phase process is based on the methodology in SP 800-53A [5][5] and includes:

1. Preparing for assessments
2. Developing assessment plans
3. Conducting assessments
4. Analyzing, documenting, and reporting assessment results

D.1. Preparing for Assessments

Thorough preparation by the organization and assessors is an important aspect of conducting an effective assessment. Preparatory activities address a range of issues related to the cost, schedule, and conduct of the assessment. From an organizational perspective, preparing for an assessment includes the following activities:

- Ensuring that appropriate policies that cover the assessment are in place and understood by affected organizational elements
- Establishing the objective and scope of the assessment (i.e., the purpose of the assessment and what is being assessed)
- Notifying appropriate organizational officials of the impending assessment and allocating the necessary resources to carry out the assessment
- Establishing appropriate communication channels among organizational officials with an interest in the assessment
- Establishing the time frame for completing the assessment and the key milestone decision points required by the organization
- Identifying and selecting the assessors who will be responsible for conducting the assessment and considering issues of assessor independence
- Providing artifacts to the assessors (e.g., policies, procedures, plans, specifications, designs, records, administrator/operator manuals, information exchange agreements, system documentation, previous assessment results, legal requirements)
- Establishing a mechanism between the organization and the assessors to minimize ambiguities or misunderstandings about the security requirements, implementation issues, and deficiencies identified during the assessment

[5] For additional detail and guidance, see SP 800-53A [5], Section 3.

Assessors begin preparing for the assessment by:

- Developing a general understanding of the organization's operations and how the scope of the assessment supports those organizational operations
- Understanding the structure of the system (i.e., the system architecture) and the security requirements being assessed
- Meeting with organizational officials to ensure that there is a common understanding of the assessment objectives and the proposed rigor and scope of the assessment
- Obtaining the artifacts needed for the assessment (e.g., policies, procedures, plans, specifications, administrator/operator manuals, system documentation, information exchange agreements, designs, records, previous assessment results[6])
- Establishing organizational points of contact to carry out the assessment

Table 3 provides a summary of the purpose and expected outcomes of the *assessment preparation phase*.

Table 3. Summary of assessment preparation phase

PURPOSE	**Address a range of issues pertaining to the cost, schedule, scope, and conduct of the assessment.**
OUTCOMES	• The objective, scope, and time frame of the assessment are determined. • Key organizational stakeholders are notified, and the necessary resources are allocated. • Assessors are identified and selected. • Artifacts are collected and provided to assessors. • Mechanisms to minimize ambiguities and misunderstandings about the security requirements, implementation issues, and weaknesses/deficiencies identified during the assessment are established. • The organization's operations, structure, objective, scope, and time frame of assessment are understood by assessors.

D.2. Developing Assessment Plans

The assessment plan establishes the objectives for the security requirement assessment and a detailed roadmap of how to conduct the assessment based on the system security plan. The following steps are considered by assessors when developing an assessment plan:

- Determine which security requirements are to be included in the assessment based on the contents of the system security plan and the purpose and scope of the assessment.
- Select the appropriate assessment procedures.

[6] Previous assessment results that may be reused for the current assessment include Inspector General reports, audits, vulnerability scans, physical security inspections, developmental testing and evaluation, vendor flaw remediation activities, and ISO 15408 [6] evaluations.

- Tailor the selected assessment procedures (i.e., select appropriate POTENTIAL ASSESSMENT METHODS AND OBJECTS, and assign depth and coverage attribute values).[7]
- Optimize the assessment procedures to reduce the duplication of effort (e.g., sequence and consolidate assessment procedures) and provide a cost-effective assessment solution.
- Finalize the assessment plan, and obtain the necessary approvals to execute the plan.

Table 4 provides a summary of the purpose and expected outcomes of the *assessment plan development phase*.

Table 4. Summary of assessment plan development phase

PURPOSE	**Establish the objectives for the security requirement assessment and a detailed roadmap of how to conduct the assessment based on the system security plan.**
OUTCOMES	• Security requirements to be included in the assessment are determined. • Assessment procedures are selected and tailored. • Assessment procedures are optimized to reduce the duplication of effort. • The assessment plan is finalized, and organizational approvals are obtained.

D.3. Conducting Assessments

After the assessment plan is approved by the organization, the assessors execute the plan in accordance with the agreed-upon schedule. Assessment objectives are achieved by applying the designated assessment methods to selected assessment objects and compiling or producing the evidence necessary to make the determination associated with each assessment objective. Each determination statement contained within an assessment procedure executed by an assessor produces one of the following findings:

- Satisfied

or

- Other than satisfied

A finding of *satisfied* indicates that the assessment objective for the security requirement (or subset of the requirement) addressed by the determination statement has been met and produced an acceptable result. A finding of *other than satisfied* indicates that the assessment objective for the requirement has not been met and has produced an unacceptable result. A

[7] In addition to selecting POTENTIAL ASSESSMENT METHODS AND OBJECTS, each assessment method (i.e., examine, interview, and test) is associated with depth and coverage attributes. The attribute values identify the rigor (depth) and scope (coverage) of the assessment procedures executed by the assessor. The depth and coverage attribute values are associated with the assurance requirements specified by the organization. SP 800-53A [5], Appendix D provides additional guidance on depth and coverage attributes.

finding of *other than satisfied* may also indicate that the assessor was unable to obtain sufficient information to make the determination called for in the determination statement.

Table 5 provides a summary of the purpose and expected outcomes of the *assessment execution phase*.

Table 5. Summary of assessment execution phase

PURPOSE	**Conduct the assessment in accordance with the assessment plan, and document the results in an assessment report.**
OUTCOMES	• Security requirements are assessed in accordance with the assessment plan. • An assessment report that documents whether the security requirements have been satisfied is produced.

D.4. Analyzing, Documenting, and Reporting Assessment Results

The assessment report includes information from assessors in the form of findings that are necessary to determine whether the requirements in SP 800-172 [3] have been satisfied.[8] The report conveys the results of the assessment to designated organizational officials. The report can also provide recommendations for correcting any deficiencies discovered during the assessment. Depending on the organization's objective for the assessment, the assessment results can trigger a variety of risk response actions, including risk acceptance, risk mitigation, risk rejection, risk transfer, or risk sharing. The assessment results can also influence changes to the system security plan and plan of action and milestones.

Table 6 provides a summary of the purpose and expected outcomes of the *assessment analysis, documentation, and reporting phase*.

Table 6. Summary of assessment analysis, documentation, and reporting phase

PURPOSE	**Analyze the risks that result from the weaknesses and deficiencies identified during the assessment, and determine an approach to respond to those risks in accordance with organizational priorities.**
OUTCOMES	• Assessment findings are reviewed and analyzed. • Subsequent risk responses are initiated to manage risks. • The system security plan and plan of action and milestones are updated to reflect the results of the assessment and any subsequent risk response actions.

[8] SP 800-53A [5], Appendix E provides additional guidance on security assessment reports.

Appendix E. Organization-Defined Parameters

Table 7 lists the ODPs that are included in the assessment procedures in Sec. 3. The ODPs are listed sequentially by requirement family, beginning with the first requirement containing an ODP in the Access Control (AC) family and ending with the last requirement containing an ODP in the Supply Chain Risk Management (SR) family.

Table 7. Organization-defined parameters

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.01.01E	A.03.01.01E.ODP[01]	*privileged commands and/or other actions requiring dual authorization are defined.*
03.01.02E	A.03.01.02E.ODP[01]	*restrictions on the use of non-organizationally owned systems or system components to process, store, or transmit CUI are defined.*
03.01.04E	A.03.01.04E.ODP[01]	*accounts and/or account types for which to limit the number of concurrent sessions is defined.*
03.01.04E	A.03.01.04E.ODP[02]	*the number of concurrent sessions to be allowed for each account and/or account type is defined.*
03.01.08E	A.03.01.08E.ODP[01]	*atypical usage for which to monitor system accounts is defined.*
03.01.08E	A.03.01.08E.ODP[02]	*personnel or roles to report atypical usage are defined.*
03.01.09E	A.03.01.09E.ODP[01]	*attributes to assume access permissions are defined.*
03.01.10E	A.03.01.10E.ODP[01]	*security attributes to be associated with information, source, and destination objects are defined.*
03.01.10E	A.03.01.10E.ODP[02]	*information objects to be associated with information security attributes are defined.*
03.01.10E	A.03.01.10E.ODP[03]	*source objects to be associated with information security attributes are defined.*
03.01.10E	A.03.01.10E.ODP[04]	*destination objects to be associated with information security attributes are defined.*
03.01.10E	A.03.01.10E.ODP[05]	*information flow control policies as a basis for the enforcement of flow control decisions are defined.*
03.01.11E	A.03.01.11E.ODP[01]	*roles and users authorized to assume such roles are defined.*
03.01.12E	A.03.01.12E.ODP[01]	*mechanisms and/or techniques to separate CUI flows are defined.*
03.01.13E	A.03.01.13E.ODP[01]	*metadata that requires flow control is defined.*
03.01.14E	A.03.01.14E.ODP[01]	*security policy filers are defined.*
03.01.14E	A.03.01.14E.ODP[02]	*information flows are defined.*
03.01.14E	A.03.01.14E.ODP[03]	*one or more of the following PARAMETER VALUES is/are selected: {Block; Strip; Modify; Quarantine} in response to a filter processing failure.*
03.01.14E	A.03.01.14E.ODP[04]	*security policy addressing a filter processing failure is defined.*
03.01.15E	A.03.01.15E.ODP[01]	*data type identifiers are defined.*
03.01.16E	A.03.01.16E.ODP[01]	*policy-relevant subcomponents into which to decompose information for submission to policy enforcement mechanisms are defined.*

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.01.17E	A.03.01.17E.ODP[01]	*unsanctioned information to be detected is defined.*
03.01.17E	A.03.01.17E.ODP[02]	*a security policy that prohibits the transfer of such information is defined.*
03.02.01E	A.03.02.01E.ODP[01]	*indicators of malicious code are defined.*
03.02.01E	A.03.02.01E.ODP[02]	*the frequency at which to update security literacy training content is defined.*
03.02.01E	A.03.02.01E.ODP[03]	*events which cause security literacy training content to be updated are defined.*
03.02.03E	A.03.02.03E.ODP[01]	*personnel to whom feedback on organizational training results will be provided are assigned.*
03.02.04E	A.03.02.04E.ODP[01]	*personnel or roles requiring training to detect counterfeit system components are defined.*
03.03.02E	A.03.03.02E.ODP[01]	*real-time period requiring alerts when audit failure events (defined in A.03.03.02E.ODP[03]) occur is defined.*
03.03.02E	A.03.03.02E.ODP[02]	*personnel, roles, and/or locations to be alerted in real time when audit failure events (defined in A.03.03.02E.ODP[03]) occur are defined.*
03.03.02E	A.03.03.02E.ODP[03]	*audit logging failure events requiring real-time alerts are defined.*
03.03.03E	A.03.03.03E.ODP[01]	*one or more of the following PARAMETER VALUES is/are selected: {movement; deletion}.*
03.03.03E	A.03.03.03E.ODP[02]	*audit information for which dual authorization is to be enforced is defined.*
03.03.04E	A.03.03.04E.ODP[01]	*one or more of the following PARAMETER VALUES is/are selected: {vulnerability scanning information; performance data; system monitoring information; <A.03.03.04E.ODP[02] data/information collected from other sources>}.*
03.03.04E	A.03.03.04E.ODP[02]	*data or information collected from other sources to be analyzed is defined (if selected).*
03.04.02E	A.03.04.02E.ODP[01]	*automated mechanisms used to detect the presence of unauthorized or misconfigured system components are defined.*
03.04.02E	A.03.04.02E.ODP[02]	*one or more of the following PARAMETER VALUES is/are selected: {disable network access by unauthorized or misconfigured system components; isolate unauthorized or misconfigured system components; notify <A.03.04.02E.ODP[03] personnel or roles>.*
03.04.02E	A.03.04.02E.ODP[03]	*personnel or roles to be notified when unauthorized or misconfigured system components are detected are defined (if selected).*
03.04.03E	A.03.04.03E.ODP[01]	*automated mechanisms used to maintain the currency of the system component inventory are defined.*
03.04.03E	A.03.04.03E.ODP[02]	*automated mechanisms used to maintain the completeness of the system component inventory are defined.*
03.04.03E	A.03.04.03E.ODP[03]	*automated mechanisms used to maintain the accuracy of the system component inventory are defined.*

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.04.03E	A.03.04.03E.ODP[04]	*automated mechanisms used to maintain the availability of the system component inventory are defined.*
03.04.04E	A.03.04.04E.ODP[01]	*automated mechanisms used to maintain the currency of the baseline configuration of the system are defined.*
03.04.04E	A.03.04.04E.ODP[02]	*automated mechanisms used to maintain the completeness of the baseline configuration of the system are defined.*
03.04.04E	A.03.04.04E.ODP[03]	*automated mechanisms used to maintain the accuracy of the baseline configuration of the system are defined.*
03.04.04E	A.03.04.04E.ODP[04]	*automated mechanisms used to maintain the availability of the baseline configuration of the system are defined.*
03.04.05E	A.03.04.05E.ODP[01]	*system components requiring dual authorization for changes are defined.*
03.04.05E	A.03.04.05E.ODP[02]	*system-level information requiring dual authorization for changes is defined.*
03.04.06E	A.03.04.06E.ODP[01]	*the number of previous baseline configuration versions to be retained is defined.*
03.05.01E	A.03.05.01E.ODP[01]	*devices and/or types of devices requiring the use of cryptographically based bidirectional authentication to authenticate before establishing a system connection are defined.*
03.05.02E	A.03.05.02E.ODP[01]	*password managers employed for generating and managing passwords are defined.*
03.05.03E	A.03.05.03E.ODP[01]	*the configuration management process to be implemented to handle device identification and authentication based on attestation is defined.*
03.05.05E	A.03.05.05E.ODP[01]	*the time period after which the use of cached authenticators is prohibited is defined.*
03.05.07E	A.03.05.07E.ODP[01]	*an identification and authentication policy is defined.*
03.05.07E	A.03.05.07E.ODP[02]	*mechanisms supporting authentication and authorization decisions are defined.*
03.06.02E	A.03.06.02E.ODP[01]	*the time period within which an integrated incident response team can be deployed is defined.*
03.06.03E	A.03.06.03E.ODP[01]	*environments or resources that may contain or be related to anomalous or suspected adversarial behavior are defined.*
03.06.04E	A.03.06.04E.ODP[01]	*automated mechanisms used to track incidents are defined.*
03.06.04E	A.03.06.04E.ODP[02]	*automated mechanisms used to collect incident information are defined.*
03.06.04E	A.03.06.04E.ODP[03]	*automated mechanisms used to analyze incident information are defined.*
03.08.01E	A.03.08.01E.ODP[01]	*system media to be sanitized using dual authorization is defined.*
03.08.02E	A.03.08.02E.ODP[01]	*backup information for which to enforce dual authorization in order to delete or destroy is defined.*
03.08.03E	A.03.08.03E.ODP[01]	*the frequency at which to test backup information for media reliability is defined.*

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.08.03E	A.03.08.03E.ODP[02]	*the frequency at which to test backup information for information integrity is defined.*
03.08.04E	A.03.08.04E.ODP[01]	*a time period consistent with recovery time and recovery point objectives for the recovery of the system is determined.*
03.08.04E	A.03.08.04E.ODP[02]	*a time period consistent with recovery time and recovery point objectives for the reconstitution of the system is determined.*
03.09.03E	A.03.09.03E.ODP[01]	*the frequency at which to review and update access agreements is defined.*
03.09.03E	A.03.09.03E.ODP[02]	*the frequency at which to re-sign access agreements to maintain access systems processing, storing, or transmitting CUI is defined.*
03.09.04E	A.03.09.04E.ODP[01]	*Citizenship requirements to be met by individuals to access a system processing, storing, or transmitting CUI are defined.*
03.10.01E	A.03.10.01E.ODP[01]	*the time period for which to maintain visitor access records for the facility in which the system resides is defined.*
03.10.02E	A.03.10.02E.ODP[01]	*the types of system components to be authorized and controlled when entering the facility are defined.*
03.10.02E	A.03.10.02E.ODP[02]	*the types of system components to be authorized and controlled when exiting the facility are defined.*
03.11.02E	A.03.11.02E.ODP[01]	*the frequency at which to implement the threat-hunting capability is defined.*
03.11.03E	A.03.11.03E.ODP[01]	*advanced automation capabilities to predict and identify risks are defined.*
03.11.03E	A.03.11.03E.ODP[02]	*systems or system components in which advanced automation and analytics capabilities are to be employed are defined.*
03.11.03E	A.03.11.03E.ODP[03]	*advanced analytics capabilities to predict and identify risks are defined.*
03.11.08E	A.03.11.08E.ODP[01]	*the means to determine the current cyber threat environment on an ongoing basis are defined.*
03.11.09E	A.03.11.09E.ODP[01]	*sources that provide indicators of compromise are defined.*
03.11.09E	A.03.11.09E.ODP[02]	*personnel or roles to whom indicators of compromise are to be distributed are defined.*
03.11.10E	A.03.11.10E.ODP[01]	*systems, system components, or system services to be analyzed for criticality are defined.*
03.11.10E	A.03.11.10E.ODP[02]	*decision points in the system development life cycle when a criticality analysis is to be performed are defined.*
03.11.11E	A.03.11.11E.ODP[01]	*corrective actions to be taken if information about the system is discoverable are defined.*
03.12.01E	A.03.12.01E.ODP[01]	*the frequency at which to conduct penetration testing on systems or system components is defined.*
03.12.01E	A.03.12.01E.ODP[02]	*systems or system components on which penetration testing is to be conducted are defined.*
03.12.04E	A.03.12.04E.ODP[01]	*system components or classes of components requiring internal connections to the system are defined.*

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.12.04E	A.03.12.04E.ODP[02]	*conditions requiring the termination of internal connections are defined.*
03.12.04E	A.03.12.04E.ODP[03]	*the frequency at which to review the continued need for each internal connection is defined.*
03.13.01E	A.03.13.01E.ODP[01]	*system components requiring a diverse set of information technologies to be used in the implementation of the system are defined.*
03.13.02E	A.03.13.02E.ODP[01]	*the techniques employed to introduce randomness into organizational operations and assets are defined.*
03.13.03E	A.03.13.03E.ODP[01]	*the concealment and misdirection techniques used to confuse and mislead adversaries potentially targeting systems are defined.*
03.13.04E	A.03.13.04E.ODP[01]	*system components to be isolated by boundary protection mechanisms are defined.*
03.13.05E	A.03.13.05E.ODP[01]	*processing and/or storage locations to be changed are defined.*
03.13.05E	A.03.13.05E.ODP[02]	*one of the following PARAMETER VALUES is selected: {<A.03.13.05E.ODP[03] frequency>; at random time intervals}.*
03.13.05E	A.03.13.05E.ODP[03]	*the frequency at which to change the location of processing and/or storage is defined (if selected).*
03.13.06E	A.03.13.06E.ODP[01]	*platform-independent applications to be included within organizational systems are defined.*
03.13.07E	A.03.13.07E.ODP[01]	*the frequency at which to change the diversity of operating systems and applications deployed using virtualization techniques is defined.*
03.13.09E	A.03.13.09E.ODP[01]	*information security tools, mechanisms, and support components to be isolated from other internal system components are defined.*
03.13.11E	A.03.13.11E.ODP[01]	*system components to be implemented with minimal functionality and information storage are defined.*
03.13.12E	A.03.13.12E.ODP[01]	*the types of denial-of-service events to be protected against or limited are defined.*
03.13.12E	A.03.13.12E.ODP[02]	*one of the following PARAMETER VALUES is selected: {protected against; limited}.*
03.13.12E	A.03.13.12E.ODP[03]	*the safeguards to prevent the denial-of-service objective by type of denial-of-service event are defined.*
03.13.13E	A.03.13.13E.ODP[01]	*connection ports or input/output devices to be disabled or removed are defined.*
03.13.13E	A.03.13.13E.ODP[02]	*one of the following PARAMETER VALUES is selected: {physically; logically}.*
03.13.13E	A.03.13.13E.ODP[03]	*systems or system components with connection ports or input/output devices to be disabled or removed are defined.*
03.13.14E	A.03.13.14E.ODP[01]	*the system, system component, or location in which a detonation chamber capability is to be employed is defined.*
03.13.15E	A.03.13.15E.ODP[01]	*one of the following PARAMETER VALUES is selected: {physically; logically}.*

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.13.15E	A.03.13.15E.ODP[02]	*critical system components and functions to be isolated are defined.*
03.13.16E	A.03.13.16E.ODP[01]	*system components to reside in separate physical or logical domains or environments based on circumstances for the physical or logical separation of components are defined.*
03.13.16E	A.03.13.16E.ODP[02]	*one of the following PARAMETER VALUES is selected: {physical; logical}.*
03.13.16E	A.03.13.16E.ODP[03]	*circumstances for the physical or logical separation of components are defined.*
03.14.01E	A.03.14.01E.ODP[01]	*software requiring integrity verification tools to be used to detect unauthorized changes is defined.*
03.14.01E	A.03.14.01E.ODP[02]	*firmware requiring integrity verification tools to be used to detect unauthorized changes is defined.*
03.14.01E	A.03.14.01E.ODP[03]	*information requiring integrity verification tools to be used to detect unauthorized changes is defined.*
03.14.01E	A.03.14.01E.ODP[04]	*actions to be taken when unauthorized changes to software are detected are defined.*
03.14.01E	A.03.14.01E.ODP[05]	*actions to be taken when unauthorized changes to firmware are detected are defined.*
03.14.01E	A.03.14.01E.ODP[06]	*actions to be taken when unauthorized changes to information are detected are defined.*
03.14.04E	A.03.14.04E.ODP[01]	*trusted sources to obtain software and data for system component and service refreshes are defined.*
03.14.05E	A.03.14.05E.ODP[01]	*one of the following PARAMETER VALUES is selected: {refresh <A.03.14.05E_ODP[02] information> <A.03.14.05E_ODP[03] frequency>; generate <A.03.14.05E_ODP[04] information>}.*
03.14.05E	A.03.14.05E.ODP[02]	*the information to be refreshed is defined (if selected).*
03.14.05E	A.03.14.05E.ODP[03]	*the frequency at which to refresh information is defined (if selected).*
03.14.05E	A.03.14.05E.ODP[04]	*the information to be generated on demand is defined (if selected).*
03.14.08E	A.03.14.08E.ODP[01]	*software on which an integrity check is to be performed is defined.*
03.14.08E	A.03.14.08E.ODP[02]	*one or more of the following PARAMETER VALUES is/are selected: {at startup; at <A.03.14.08E.ODP[03] transitional states or security-relevant events>; <A.03.14.08E.ODP[04] frequency>}.*
03.14.08E	A.03.14.08E.ODP[03]	*transitional states or security-relevant events requiring integrity checks (on software) are defined (if selected).*
03.14.08E	A.03.14.08E.ODP[04]	*the frequency at which to perform an integrity check (on software) is defined (if selected).*
03.14.08E	A.03.14.08E.ODP[05]	*firmware on which an integrity check is to be performed is defined.*

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.14.08E	A.03.14.08E.ODP[06]	*one or more of the following PARAMETER VALUES is/are selected: {at startup; at <A.03.14.08E.ODP[07] transitional states or security-relevant events>; <A.03.14.08E.ODP[08] frequency>}.*
03.14.08E	A.03.14.08E.ODP[07]	*transitional states or security-relevant events requiring integrity checks (on firmware) are defined (if selected).*
03.14.08E	A.03.14.08E.ODP[08]	*the frequency at which to perform an integrity check (on firmware) is defined (if selected).*
03.14.08E	A.03.14.08E.ODP[09]	*information on which an integrity check is to be performed is defined.*
03.14.08E	A.03.14.08E.ODP[10]	*one or more of the following PARAMETER VALUES is/are selected: {at startup; at <A.03.14.08E.ODP[11] transitional states or security-relevant events>; <A.03.14.08E.ODP[12] frequency>}.*
03.14.08E	A.03.14.08E.ODP[11]	*transitional states or security-relevant events requiring integrity checks (of information) are defined (if selected).*
03.14.08E	A.03.14.08E.ODP[12]	*the frequency at which to perform an integrity check (of information) is defined (if selected).*
03.14.10E	A.03.14.10E.ODP[01]	*mechanisms to be implemented to protect the integrity of boot firmware in system components are defined.*
03.14.10E	A.03.14.10E.ODP[02]	*system components requiring mechanisms to protect the integrity of boot firmware are defined.*
03.14.11E	A.03.14.11E.ODP[01]	*security-relevant changes to the system are defined.*
03.14.12E	A.03.14.12E.ODP[01]	*information inputs to the system requiring validity checks are defined.*
03.14.13E	A.03.14.13E.ODP[01]	*personnel or roles to whom error messages are to be revealed are defined.*
03.14.14E	A.03.14.14E.ODP[01]	*safeguards to be implemented to protect the system memory from unauthorized code execution are defined.*
03.14.15E	A.03.14.15E.ODP[01]	*non-persistent system components and services to be implemented are defined.*
03.14.15E	A.03.14.15E.ODP[02]	*one or more of the following PARAMETER VALUES is/are selected: {upon end of session of use; <A.03.14.15E.ODP[03] frequency>}.*
03.14.15E	A.03.14.15E.ODP[03]	*the frequency at which to terminate non-persistent components and services that are initiated in a known state is defined (if selected).*
03.14.16E	A.03.14.16E.ODP[01]	*systems or system components with data or capabilities to be embedded are defined.*
03.14.17E	A.03.14.17E.ODP[01]	*personnel or roles to be alerted when indications of compromise or potential compromise occur are defined.*
03.14.17E	A.03.14.17E.ODP[02]	*compromise indicators are defined.*
03.14.18E	A.03.14.18E.ODP[01]	*personnel or roles to be alerted when indications of inappropriate or unusual activity with security implications occur are defined.*
03.14.18E	A.03.14.18E.ODP[02]	*automated mechanisms used to alert personnel or roles are defined.*
03.14.18E	A.03.14.18E.ODP[03]	*activities that trigger alerts to personnel or roles are defined.*

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.15.01E	A.03.15.01E.ODP[01]	*the frequency for reviewing and updating the security architecture to reflect changes in the enterprise architecture is defined.*
03.15.02E	A.03.15.02E.ODP[01]	*safeguards to be allocated to architectural layers and locations are defined.*
03.15.02E	A.03.15.02E.ODP[02]	*architectural layers and locations are defined.*
03.15.03E	A.03.15.03E.ODP[01]	*safeguards to be allocated to architectural layers and locations are defined.*
03.15.03E	A.03.15.03E.ODP[02]	*architectural layers and locations are defined.*
03.16.01E	A.03.16.01E.ODP[01]	*one or more of the following PARAMETER VALUES is/are selected: {design modification; augmentation; reconfiguration}.*
03.16.01E	A.03.16.01E.ODP[02]	*systems or system components supporting mission-essential services or functions are defined.*
03.17.01E	A.03.17.01E.ODP[01]	*one or more of the following PARAMETER VALUES is/are selected: {notification of supply chain compromises; results of assessments or audits; provision of <A.03.17.01E.ODP[02]: information>}.*
03.17.01E	A.03.17.01E.ODP[02]	*information for which agreements and procedures are to be established is defined (if selected).*
03.17.02E	A.03.17.02E.ODP[01]	*systems or system components that require inspection are defined.*
03.17.02E	A.03.17.02E.ODP[02]	*one or more of the following PARAMETER VALUES is/are selected: {at random; <A.03.17.02E.ODP[03]: frequency>; upon <A.03.17.02E.ODP[04]: indications of the need for inspection>}.*
03.17.02E	A.03.17.02E.ODP[03]	*the frequency at which to inspect systems or system components is defined (if selected).*
03.17.02E	A.03.17.02E.ODP[04]	*indications of the need for an inspection of systems or system components are defined (if selected).*
03.17.03E	A.03.17.03E.ODP[01]	*one or more of the following PARAMETER VALUES is/are selected: {source of counterfeit component; <A.03.17.03E.ODP[02]: external reporting organizations>; <A.03.17.03E.ODP[03]: personnel or roles>}.*
03.17.03E	A.03.17.03E.ODP[02]	*external reporting organizations to whom counterfeit system components are to be reported are defined (if selected).*
03.17.03E	A.03.17.03E.ODP[03]	*personnel or roles to whom counterfeit system components are to be reported are defined (if selected).*
03.17.04E	A.03.17.04E.ODP[01]	*systems, system components, and associated CUI that require valid provenance are defined.*
03.17.05E	A.03.17.05E.ODP[01]	*safeguards employed to ensure the integrity of the system and system component are defined.*
03.17.05E	A.03.17.05E.ODP[02]	*an analysis method to be conducted to validate the internal composition and provenance of critical or mission-essential technologies, products, and services to ensure the integrity of the system and system component is defined.*

3250

Appendix F. Change Log

This publication incorporates the following changes from the original edition (March 15, 2022):

- The restructuring of the assessment procedure syntax to align with SP 800-53A [5]
- The addition of assessment procedures for the new and revised enhanced security requirements in SP 800-172, Revision 3 [3]
- The addition of a references section to provide source assessment procedures from SP 800-53A [5]
- A one-time change to the publication version number to align with SP 800-172, Revision 3 [3]