NIST Special Publication 800
NIST SP 800-172r3 ipd

Enhanced Security Requirements for Protecting 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.800-172r3.ipd

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

NIST Special Publication 800
NIST SP 800-172r3 ipd

Enhanced Security Requirements for Protecting 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.800-172r3.ipd

November 2024

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

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

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. 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.

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 (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

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

Public Comment Period
November 13, 2024 – January 10, 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

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/172/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 recommended security requirements for protecting the confidentiality, integrity, and availability of CUI when it is resident in a nonfederal system and organization and associated with a critical program or high value asset (HVA). The security requirements apply to the components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components. The enhanced security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

Keywords

advanced persistent threat; contractor systems; controlled unclassified information; CUI registry; enhanced security requirement; Executive Order 13556; FISMA; NIST Special Publication 800-172; NIST Special Publication 800-53; nonfederal organizations; nonfederal systems; security assessment; security control; security requirement.

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

This update to NIST Special Publication (SP) 800-172 represents over one year of data collection, technical analysis, customer interaction, and the redesign and development of enhanced security requirements and supporting information for the protection of Controlled Unclassified Information (CUI) associated with critical programs and high value assets. Many trade-offs have been made to ensure that the technical and non-technical requirements have been stated clearly and concisely while recognizing the specific needs of both federal and nonfederal organizations. The following provides a summary of the significant changes that have been made to SP 800-172 in transitioning to Revision 3:

- Streamlined introductory information in Sec. 1 and Sec. 2 to improve clarity and understanding
- Increased specificity of the enhanced security requirements to remove ambiguity, improve the effectiveness of implementation, and clarify the scope of assessments
- Grouped enhanced security requirements, where possible, to improve understanding and the efficiency of implementations and assessments
- Removed outdated and redundant enhanced security requirements
- Added new enhanced security requirements based on (1) the latest threat intelligence, (2) empirical data from cyber-attacks, and (3) the expansion of security objectives to include integrity and availability
- Added new requirement families for consistency with SP 800-171r3, Revision 3: Planning (PL), System and Services Acquisition (SA), and Supply Chain Risk Management (SR)
- Added titles to the enhanced security requirements
- Restructured and streamlined the security requirement discussion sections
- Revised the enhanced security requirements for consistency with the source security control language in SP 800-53
- Revised the structure of the References, Acronyms, and Glossary sections for greater clarity and ease of use
- Removed appendix with mapping table for security controls and protection strategies and transferred information to the individual security requirements in Sec. 3
- Added new appendix that summarizes the enhanced security requirements
- Added new appendix that lists organization-defined parameters for the enhanced security requirements
- Implemented a one-time “revision number” change for consistency with SP 800-171r3

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 Figures

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. In particular, the authors wish to thank Jeffrey Eyink from the Department of Defense (DOD) Chief Information Office for his contributions to this update. The authors also wish to thank the NIST technical editing and production staff – Jim Foti, Jeff Brewer, Eduardo Takamura, Isabel Van Wyk, and Cristina Ritfeld – for their outstanding support in preparing this document for publication.

Historical Contributions

The authors also wish to acknowledge the following organizations and individuals for their historic contributions to this publication:

- *Organizations:* Department of Defense, Institute for Defense Analyses, The MITRE Corporation
- *Individuals:* Gary Guissanie, Ryan Wagner, Richard Graubart, Deb Bodeau

1. Introduction

Executive Order (EO) 13556 [1] established a government-wide program to standardize how the executive branch handles Controlled Unclassified Information (CUI).[1] EO 13556 required that the CUI program emphasize government-wide openness, transparency, and uniformity and that the program implementation take place in a manner consistent with Office of Management and Budget (OMB) policies and National Institute of Standards and Technology (NIST) standards and guidelines. The National Archives and Records Administration (NARA), as the CUI program Executive Agent, provides information, guidance, policy, and requirements on handling CUI [4]. This includes approved CUI categories and category descriptions, the basis for safeguarding and dissemination controls, and procedures for the use of CUI.[2] The CUI federal regulation [5] provides guidance to federal agencies on the designation, safeguarding, marking, dissemination, decontrolling, and disposition of CUI; establishes self-inspection and oversight requirements; and delineates other facets of the program.

The CUI regulation requires federal agencies that use federal information systems[3] to process, store, or transmit CUI to comply with NIST standards and guidelines. The responsibility of federal agencies to protect CUI does not change when such information is shared with nonfederal organizations.[4] Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by nonfederal organizations using nonfederal systems. The requirements for protecting CUI in nonfederal systems and organizations must comply with Federal Information Processing Standards (FIPS) 199 [6] and FIPS 200 [7] to maintain a consistent level of protection. The requirements are derived from the controls in NIST Special Publication (SP) 800-53 [8].

In certain situations, CUI may be associated with a critical program[5] or a high value asset.[6] These programs and assets are potential targets for the advanced persistent threat (APT). An APT is an adversary or adversarial group that possesses the expertise and resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception. APT objectives include establishing a foothold within the infrastructure of targeted organizations exfiltrate information; undermine or impede critical aspects of a mission, function, program, or organization; or position itself to carry out these objectives in the future. The APT pursues its objectives repeatedly over an extended period, adapts to defenders' efforts to resist it, and is determined to maintain the interaction needed

[1] CUI is any information that a law, regulation, or government-wide policy requires to have safeguarding or dissemination controls, excluding information that is classified under EO 13526 [2], or any predecessor or successor order, or the Atomic Energy Act [3] as amended.

[2] Procedures for the use of CUI include marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.

[3] A *federal information system* is a system that is used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. Any system that does not meet the definition of a federal information system is designated as a *nonfederal system*.

[4] A *nonfederal organization* is any entity that owns, operates, or maintains a nonfederal system.

[5] The definition of a critical program may vary from organization to organization. For example, the Department of Defense defines a critical program as one that significantly increases capabilities and mission effectiveness or extends the expected effective life of an essential system or capability [9].

[6] See OMB Memorandum M-19-03 [10].

to execute its objectives. CUI associated with critical programs or high value assets is at increased risk and requires additional protection because the APT is likely to target such information.

The APT is dangerous to the national and economic security interests of the United States since organizations depend on systems[7] of all types, including information technology (IT) systems, operational technology (OT) systems, and (3) Internet of Things (IoT) devices. The convergence of these types of systems and devices has brought forth a new class of systems known as *cyber-physical systems*, many of which are in sectors of United States critical infrastructure, including energy, transportation, defense, manufacturing, healthcare, finance, and information and communications. Therefore, CUI that is processed, stored, or transmitted by any of the above systems related to a critical program or high value asset requires additional protection from the APT.

1.1. Purpose and Applicability

This publication provides federal agencies with a set of recommended enhanced security requirements[8] for protecting the *confidentiality*, *integrity*, and *availability* of CUI when such information is resident in nonfederal systems and organizations and where there are no specific safeguarding requirements prescribed by the authorizing law, regulation, or government-wide policy for the CUI category listed in the CUI registry [4].[9] The enhanced security requirements address the protection of CUI by promoting penetration-resistant architecture, damage-limiting operations, and cyber resiliency.[10] The requirements supplement the requirements in SP 800-171 [12] and apply to components[11] of nonfederal systems that process, store, or transmit CUI associated with a critical program or a high value asset or that provide protection for such components. The requirements are intended for use by federal agencies in contractual vehicles or other agreements that are established between those agencies and nonfederal organizations.

Appropriately scoping security requirements is an important factor in determining protection-related investment decisions and managing security risks for nonfederal organizations. If nonfederal organizations designate specific system components to process, store, or transmit CUI associated with a critical program or a high value asset, those organizations may limit the scope of the security requirements by isolating the system components in a separate CUI

[7] The term "system" is used in this publication to represent people, processes, and technologies that are involved in the processing, storage, or transmission of CUI.

[8] The term "requirements" is used in this guideline to describe the stakeholder protection needs of a particular system or organization. Stakeholder protection needs and corresponding security requirements may be derived from many sources (e.g., laws, Executive Orders, directives, regulations, policies, standards, mission and business needs, or risk assessments).

[9] Nonfederal organizations that collect or maintain information on behalf of a federal agency or that use or operate a system on behalf of an agency must comply with the requirements in FISMA [11].

[10] Protecting the integrity and availability of the means used to achieve confidentiality protection is within the scope of this publication. While outside of the explicit purpose of this publication, the APT may seek to harm organizations, individuals, or the Nation by compromising the integrity and availability of CUI upon which mission and business functions depend, such as software that is categorized as CUI.

[11] System *components* include workstations, servers, notebook computers, smartphones, tablets, input and output devices, operating systems, network components, virtual machines, database management systems, and applications.

security domain. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for CUI and avoid increasing the organization's security posture beyond what it requires to protect its missions, functions, operations, and assets.

This publication does not provide guidance on which organizational programs or assets are determined to be critical or of high value. Those determinations are made by the federal agencies mandating the use of the security requirements for additional protection and can be guided and informed by laws, Executive Orders, directives, regulations, or policies. Additionally, this publication does not provide guidance on specific types of threats or attack scenarios that justify the use of the security requirements. Finally, there is no expectation that all of the security requirements will be needed in every situation. Rather, requirements are selected by federal agencies based on mission needs and risk.

1.2. Organization of This Publication

The remainder of this publication is organized as follows:

- Section 2 describes the assumptions and methodology used to develop the enhanced security requirements and the organization and structure of the requirements.
- Section 3 lists the enhanced security requirements for protecting the confidentiality, integrity, and availability of CUI in nonfederal systems and organizations.

The following sections provide additional information to support the protection of CUI:

- References
- Appendix A: Acronyms
- Appendix B: Glossary
- Appendix C: Summary of Enhanced Security Requirements
- Appendix D: Adversary Effects
- Appendix E: Organization-Defined Parameters
- Appendix F: Change Log

2. The Fundamentals

This section describes the assumptions and methodology used to develop the enhanced security requirements for nonfederal systems and organizations to protect the confidentiality, integrity, and availability of CUI associated with critical systems or high value assets.

2.1. Enhanced Security Requirement Assumptions

The enhanced security requirements in this publication are based on the following assumptions:

- Federal information that is designated as CUI has the same value whether such information resides in a federal or nonfederal system or organization.
- Statutory and regulatory requirements for the protection of CUI are consistent in federal and nonfederal systems and organizations.
- Safeguards implemented to protect CUI are consistent in federal and nonfederal systems and organizations.
- The impact value for CUI is no less than *moderate*.[12]
- The security requirements in SP 800-171 [12] have been satisfied to provide the foundational level of protection for CUI.
- Additional safeguards are necessary to protect CUI that is associated with critical programs or high value assets.[13]
- Nonfederal organizations can directly implement a variety of potential security solutions or use external service providers to satisfy the security requirements.

2.2. Enhanced Security Requirement Development Methodology

The enhanced security requirements provide the capability to achieve a multidimensional, defense-in-depth protection strategy [13] that includes:

- *Penetration-resistant architecture:* An architecture that uses technology and procedures to limit the opportunities for an adversary to compromise an organizational system and to achieve a persistent presence in the system.
- *Damage-limiting operations:* Procedural and operational measures that use system capabilities to maximize the ability of an organization to detect successful system compromises by an adversary and to limit the effects of such compromises (both detected and undetected).

[12] In accordance with 32 CFR 2002 [5], CUI is categorized at no less than the FIPS 199 [6] moderate confidentiality impact value. However, when federal law, regulation, or government-wide policy establishing the control of CUI specifies controls that differ from those of the moderate control baseline, then the applicable law, regulation, or government-wide policy is followed.

[13] Additional protections are required to protect CUI that is associated with critical programs and high value assets because such information is more likely to be targeted by the APT and is, therefore, at greater risk.

- *Cyber resiliency:* The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable organizational missions or business objectives that depend on cyber resources to be achieved in a contested cyber environment.

This strategy recognizes that the APT may find ways to compromise established defenses despite the best safeguards implemented by organizations. When this occurs, organizations must have access to additional safeguards to detect, outmaneuver, confuse, deceive, mislead, and impede the adversary—that is, removing the adversary's tactical advantage and protecting the organization's critical programs and high value assets. Figure 1 shows the complementary nature of the enhanced security requirements when they are implemented as part of a multidimensional protection strategy.

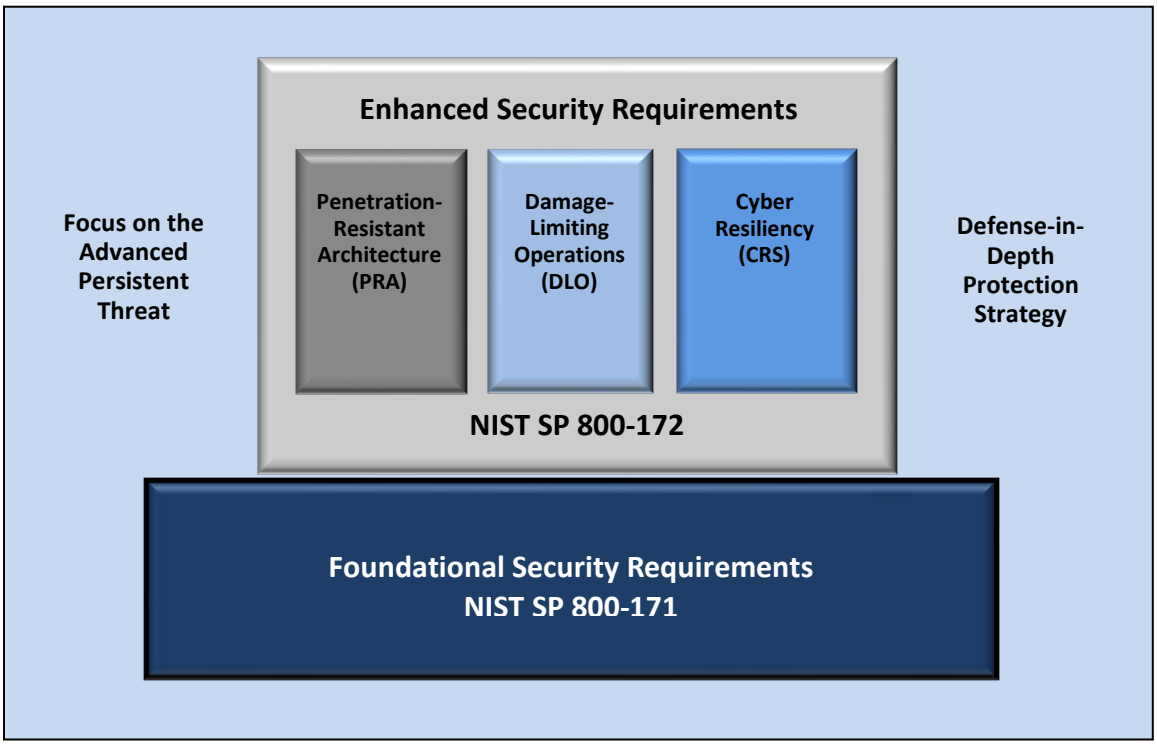

Fig. 1. Multidimensional protection strategy

The enhanced security requirements are derived from the security controls and control enhancements in SP 800-53 [8]. The requirements address safeguards to protect CUI from the APT and ensure the cyber resiliency of systems and organizations. The security requirements focus on the following key elements, which are essential to addressing the APT:

- Applying a threat-centric approach to security requirement specification
- Employing system and security architectures that support logical and physical isolation using system and network segmentation techniques, virtual machines, and containers

- Implementing dual authorization controls for critical or sensitive operations
- Limiting persistent storage to isolated enclaves or domains
- Implementing a comply-to-connect approach for systems and networks
- Extending configuration management requirements by establishing authoritative sources for addressing changes to systems and system components
- Periodically refreshing or upgrading organizational systems and system components to a known state or developing new systems or components
- Employing a security operations center with advanced analytics to support continuous monitoring and the protection of systems
- Using deception to confuse and mislead adversaries regarding the information they use for decision-making, the value and authenticity of the information they attempt to exfiltrate, or the environment in which they are operating

Similar to the security requirements in SP 800-171 [12], the enhanced security requirements 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

Each family contains the security requirements related to the general security topic of the family.[14] The structure of the security requirements is the same as the requirements in SP 800-171 [12]. The enhanced security requirements are distinguished from the security requirements in SP 800-171 by appending the letter "E" to the requirement numbers.

Organization-defined parameters (ODPs) are used in certain enhanced security requirements. ODPs provide flexibility through the use of *assignment* and *selection* operations to allow federal agencies and nonfederal organizations to specify values for the designated parameters in the requirements.[15] Assignment and selection operations provide the capability to customize the enhanced security requirements based on specific protection needs. The determination of ODP values can be guided and informed by laws, Executive Orders, directives, regulations, policies, standards, guidance, or mission and business needs. Once specified, the values for the ODPs become part of the requirement.

[14] Certain enhanced security requirements may not align with the families in SP 800-53 [8].

[15] NIST does not establish or assign values for ODPs. If ODP values for selected security requirements are not formally established or assigned by a federal agency or a consortium of federal agencies, nonfederal organizations must assign those values to complete the requirements.

A *discussion* section is included with each requirement. It is derived from the control discussion section in SP 800-53 [8] and provides additional information to facilitate the implementation and assessment of the requirement. The discussion section is informative, not normative. It is not intended to extend the scope of a requirement or influence the solutions that organizations may implement to satisfy a requirement. The use of examples is notional, not exhaustive, and does not reflect the potential options available to organizations. If applicable, the security requirement in SP 800-171 [12] that is enhanced by the requirement is noted in this section.

A *protection strategy* section describes which of the three elements of the multidimensional protection strategy (i.e., penetration-resistant architecture [PRA], damage-limiting operations [DLO], and cyber resiliency [CRS]) are addressed by the enhanced security requirement.

An *adversary effects* section describes the potential effects of implementing the enhanced security requirement on risk, specifically by reducing the likelihood of the occurrence of threat events, the ability of threat events to cause harm, and the extent of that harm. Five desired effects on the adversary can be identified: *redirect*, *preclude*, *impede*, *limit*, and *expose*. Each adversary effect is further decomposed to include specific impacts on risk and expected results. The adversary effects are described in SP 800-160v2, (Volume 2) [13] and in Appendix D.

Finally, a *references* section lists the source controls[16] from SP 800-53 [8] that are associated with the enhanced security requirement. The hyperlink associated with each control provides access to the NIST Cybersecurity and Privacy Reference Tool (CPRT), which includes references to a variety of supporting technical publications. The structure and content of an enhanced security requirement is provided in the example below.

03.13.08E Decoys

Use components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.

DISCUSSION

Decoys (i.e., honeypots, honeynets, or deception nets) are established to attract adversaries and deflect attacks away from the operational systems that support organizational missions and business functions. The use of decoys requires some supporting isolation measures to ensure that any deflected malicious code does not infect organizational systems.

PROTECTION STRATEGY

DLO, CRS

ADVERSARY EFFECTS

Expose (Detect), Limit (Reduce)

REFERENCES

Source Control: SC-26

[16] With few exceptions, the security controls in SP 800-53 [8] are policy-, technology-, and sector-neutral, meaning that the controls focus on the fundamental measures necessary to protect information across the information life cycle.

2.3. Enhanced Security Requirement Selection

Organizations[17] can select the enhanced security requirements either comprehensively or selectively as part of their overarching risk management strategy. However, there are dependencies among certain requirements that may affect the selection process. The decision to select specific enhanced security requirements is based on the mission and business needs of the federal agency, group of agencies, or the Federal Government (i.e., federal entity) and is guided and informed by ongoing assessments of risk.

Federal agencies may limit application as long as the needed protection is achieved, such as by applying the enhanced security requirements to the components of nonfederal systems that process, store, or transmit CUI that is associated with a critical program or high value asset; provide protection for such components; or provide a direct attack path to such components (e.g., due to established trust relationships between system components).[18]

The security requirements for a nonfederal system processing, storing, or transmitting CUI that is associated with a critical program or a high value asset are conveyed to the nonfederal organization by the federal entity in a contract, grant, or other agreement. The implementation guidance associated with the security requirements is beyond the scope of this publication. Organizations have flexibility in the methods, techniques, technologies, and approaches used to satisfy the requirements.[19]

[17] The term "organization" is context-dependent. For example, in an enhanced security requirement with an ODP, organization can refer to the federal agency or the nonfederal organization that establishes the parameter values for the requirement.

[18] System components include mainframes, workstations, servers, input and output devices, network components, operating systems, virtual machines, applications, cyber-physical components (e.g., programmable logic controllers [PLC] or medical devices), and mobile devices (e.g., smartphones and tablets).

[19] Implementation guidance can be included in the contractual vehicles or other agreements established between federal agencies and nonfederal organizations.

3. The Requirements

This section describes enhanced security requirements that are designed to protect the confidentiality, integrity, and availability of CUI in nonfederal systems and organizations. The enhanced security requirements are not required for any particular category or article of CUI. However, if a federal agency determines that CUI is associated with a critical program or a high value asset, the CUI and the system that processes, stores, or transmits such information are potential targets for the APT and, therefore, may require increased protection. Such protection is expressed through the enhanced security requirements and is mandated by a federal agency in a contract, grant, or other agreement. The enhanced security requirements are selected either comprehensively or selectively in addition to the foundational requirements in SP 800-171 [12].

Enhanced security requirements support one or more protection strategies with potential effects on adversaries. The strategies and adversary effects are included in the supplementary information for each enhanced security requirement to assist organizations in ascertaining whether the requirement is appropriate. Ideally, the selected requirements should be balanced across the three protection strategies. Selecting requirements that fall exclusively in one area could result in an unbalanced response strategy for dealing with the APT. Similarly, with regard to potential effects on adversaries, organizations should attempt to have as broad a set of effects on an adversary as possible, given their specific missions or business objectives.

ENHANCED SECURITY REQUIREMENT ASSESSMENT

SP 800-172A provides a set of procedures to assess the security requirements described in this publication. The assessment procedures are based on the procedures described in SP 800-53A [15].

Note: Draft SP 800-172Ar3 (Revision 3) will be released with the final public draft of SP 800-172r3.

3.1. Access Control

03.01.01E Dual Authorization for Commands and Actions

Enforce dual authorization for [*Assignment: organization-defined privileged commands and/or other organization-defined actions*].

DISCUSSION

Dual authorization is also known as two-person control. Dual authorization reduces risk related to insider threats, including adversaries who have obtained credentials. Dual authorization requires the approval of two authorized individuals to execute privileged commands and/or other organizational actions that may affect the protection of CUI. To reduce the risk of collusion, organizations consider rotating

dual authorization duties to other individuals. Organizations also consider the risk associated with implementing dual authorization when immediate responses are necessary to ensure public and environmental safety. This requirement enhances SP 800-171 requirement 03.01.02.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: AC-03(02)

03.01.02E Non-Organizationally Owned Systems Restricted Use

Restrict the use of non-organizationally owned systems or system components to process, store, or transmit CUI using [*Assignment: organization-defined restrictions*].

DISCUSSION

Non-organizationally owned systems or system components include systems or system components owned by other organizations as well as personally owned devices. There are potential risks to using non-organizationally owned systems or components. In some cases, the risk is sufficiently high as to prohibit such use. In other cases, the use of such systems or system components may be allowed but restricted in some way. Restrictions include requiring the implementation of approved safeguards prior to authorizing the connection of non-organizationally owned systems and components; limiting access to types of information, services, or applications; using virtualization techniques to limit processing and storage activities to servers or system components provisioned by the organization; and agreeing to the terms and conditions for usage. This requirement enhances SP 800-171 requirement 03.01.20.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Contain, Exert)

REFERENCES

Source Control: 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

Limit the number of concurrent sessions for each [*Assignment: organization-defined account and/or account type*] to [*Assignment: organization-defined number*].

DISCUSSION

Organizations may define the maximum number of concurrent sessions for system accounts globally, by account type, by account, or any combination thereof. For example, organizations may limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications. Concurrent session control addresses concurrent sessions for system accounts. It does not, however, address concurrent sessions by single users via multiple system accounts.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Contain, Exert)

REFERENCES

Source Control: AC-10

03.01.05E Remote Access Monitoring and Control

Implement automated mechanisms to monitor and control remote access methods.

DISCUSSION

Monitoring and controlling remote access methods allows organizations to detect attacks and ensure compliance with remote access policies. This is accomplished by auditing the connection activities of remote users on system components, including servers, notebook computers, workstations, smart phones, tablets, and wearables. This requirement enhances SP 800-171 requirement 03.01.02.

PROTECTION STRATEGY

PRA, DLO

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: AC-17(01)

03.01.06E Protection of Remote Access Mechanism Information

Protect information about remote access mechanisms from unauthorized use and disclosure.

DISCUSSION

Access to organizational information about remote access mechanisms by non-organizational entities can increase the risk of unauthorized use and disclosure. The organization considers including remote access requirements in the information exchange agreements with other organizations, as applicable. Remote access requirements can also be included in rules of behavior and access agreements. This requirement enhances SP 800-171 requirement 03.01.02.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: AC-17(06)

03.01.07E Automated Actions for Account Management

Use automated mechanisms to audit account creation, modification, enabling, disabling, and removal actions.

DISCUSSION

The use of automated mechanisms to audit account management activities provides more timely and comprehensive data to guide and inform needed actions by system administrators. This requirement enhances SP 800-171 requirement 03.01.01.

PROTECTION STRATEGY

PRA, DLO

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: AC-02(04)

03.01.08E Account Monitoring for Atypical Usage

a. Monitor system accounts for [*Assignment: organization-defined atypical usage*].

b. Report atypical usage of system accounts to [*Assignment: organization-defined personnel or roles*].

DISCUSSION

Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress. This requirement enhances SP 800-171 requirement 03.01.01.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Expose (Detect)

REFERENCES

Source Control: AC-02(12)

03.01.09E Attribute-Based Access Control

Enforce attribute-based access control policy over defined subjects and objects and control access based upon [*Assignment: organization-defined attributes to assume access permissions*].

DISCUSSION

Attribute-based access control is an access control policy that restricts system access to authorized users based on specified organizational attributes (e.g., job function, identity), action attributes (e.g., read, write, delete), environmental attributes (e.g., time of day, location), and resource attributes (e.g., classification of a document). Organizations can create rules based on specified attributes and the authorizations (i.e., privileges) to perform needed operations on the systems associated with organization-defined attributes and rules. When users are assigned to attributes defined in attribute-based access control policies or rules, they can be provisioned to a system with the appropriate privileges or dynamically granted access to a protected resource. Attribute-based access control can be implemented as either a

mandatory or discretionary form of access control. This requirement enhances SP 800-171 requirement 03.01.02.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: AC-03(13)

03.01.10E Object Security Attributes

Use [*Assignment: organization-defined security attributes*] associated with [*Assignment: organization-defined information, source, and destination objects*] to enforce [*Assignment: organization-defined information flow control policies*] as a basis for flow control decisions.

DISCUSSION

Organizations implement information flow control policies and enforcement mechanisms to control the flow of CUI between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Information flow enforcement mechanisms compare the security attributes associated with information (i.e., data content and structure) and source and destination objects and respond appropriately when the enforcement mechanisms encounter information flows that are not explicitly allowed by information flow policies. Security attributes can also include source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit security attributes can be used, for example, to control the release of certain types of information. This requirement enhances SP 800-171 requirement 03.01.03.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: AC-04(01)

3.2. Awareness and Training

03.02.01E Advanced Literacy and Awareness Training

a. Provide security literacy training to system users:
   1. On the advanced persistent threat,
   2. On recognizing suspicious communications and anomalous behavior in systems using [*Assignment: organization-defined indicators of malicious code*], and
   3. On the cyber threat environment.

b. Update security literacy training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

DISCUSSION

An effective way to detect APTs, address the cyber threat environment, and preclude successful attacks is to provide specific literacy training for individuals. Threat literacy training includes educating individuals on the various ways that APTs can infiltrate the organization (e.g., through websites, emails, pop-ups, articles, and social engineering) and describes techniques for recognizing suspicious emails, the use of removable systems in non-secure settings, and the potential targeting of individuals at home. Personnel are also trained on what constitutes suspicious communications and how to respond to such communications. Training personnel on how to recognize anomalous behaviors in systems can provide organizations with early warning of the presence of malicious code. Recognizing anomalous behavior in systems can supplement the malicious code detection and protection tools and systems used by organizations. This requirement enhances SP 800-171 requirement 03.02.01.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Preclude (Preempt), Expose (Detect)

REFERENCES

Source Controls: AT-02(04), AT-02(05), AT-02(06)

03.02.02E Literacy and Awareness Training Practical Exercises

Provide practical exercises in literacy training that simulate events and incidents.

DISCUSSION

Practical exercises include no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking malicious web links via spear phishing attacks. Since threats continue to change over time, threat literacy training is dynamic. Moreover, threat literacy training is not performed in isolation from the system operations that support organizational missions and business functions. This requirement enhances SP 800-171 requirement 03.02.01.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Preclude (Preempt), Expose (Detect)

REFERENCES

Source Control: AT-02(01)

03.02.03E Literacy and Awareness Training Feedback

Provide feedback on organizational training results to the following personnel [*Assignment: organization-defined personnel*].

DISCUSSION

Training feedback includes literacy and role-based training results, which can indicate a potentially serious problem, especially the failures of personnel in critical roles. Managers should be made aware of such situations so that they can respond accordingly. Training feedback supports the evaluation and update of organizational training content and methodology.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Preclude (Preempt), Expose (Detect)

REFERENCES

Source Control: AT-06

03.02.04E Anti-Counterfeit Training

Provide training to [*Assignment: organization-defined personnel or roles*] to detect counterfeit system components.

DISCUSSION

System components include hardware, software, and firmware components, as well as the documentation for those components.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Preclude (Preempt), Expose (Detect)

REFERENCES

Source Control: SR-11(01)

3.3. Audit and Accountability

03.03.01E Audit Record Storage in Separate Environment

Store audit records in a repository that is part of a physically different system or system component than the system or component being audited.

DISCUSSION

Storing audit records in a repository that is separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components preserves the confidentiality, integrity, and availability of audit records and facilitates the management of audit records as an organization-wide activity. Storing audit records on separate systems or system components applies to the initial generation and backup or long-term storage of audit records. This requirement enhances SP 800-171 requirement 03.03.08.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: AU-09(02)

03.03.02E Real-Time Alerts for Audit Processing Failures

Provide an alert within [*Assignment: organization-defined real-time period*] to [*Assignment: organization-defined personnel, roles, and/or locations*] when the following audit failure events occur: [*Assignment: organization-defined audit logging failure events requiring real-time alerts*].

DISCUSSION

Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less). This requirement enhances SP 800-171 requirement 03.03.04.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: AU-05(02)

03.03.03E Dual Authorization for Audit Information and Actions

Enforce dual authorization for [*Selection (one or more): movement; deletion*] of [*Assignment: organization-defined audit information*].

DISCUSSION

Dual authorization is also known as two-person control since it requires the approval of two authorized individuals to execute audit functions. Dual authorization reduces risks related to insider threats, including adversaries who have obtained credentials. Organizations may choose different selection options for different types of audit information. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. Organizations consider the risk associated with implementing dual authorization when immediate responses are necessary to ensure public and environmental safety. This requirement enhances SP 800-171 requirement 03.03.08.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: AU-09(05)

03.03.04E Integrated Analysis of Audit Records

Integrate analysis of audit records with analysis of [*Selection (one or more): vulnerability scanning information; performance data; system monitoring information;* [*Assignment: organization-defined data/information collected from other sources*]] to further enhance the ability to identify inappropriate or unusual activity.

DISCUSSION

Integrated analysis of audit records requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. Security information and event management (SIEM) tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches to analyzing audit record information. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans of the system and in correlating attack detection events with scanning results. Correlation with performance data can uncover denial-of-service (DoS) attacks or other types of attacks that result in the unauthorized use of resources. Correlation with system monitoring information can also assist in uncovering attacks and relating audit information to operational situations. This requirement enhances SP 800-171 requirement 03.03.05.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Preclude (Preempt), Expose (Detect)

REFERENCES

Source Control: AU-06(05)

3.4. Configuration Management

03.04.01E Withdrawn

Addressed by 03.14.04E, 03.17.03E, 03.04.01, 03.04.03, and 03.04.10.

03.04.02E Automated Unauthorized or Misconfigured Component Detection

a. Detect the presence of unauthorized or misconfigured system components using [*Assignment: organization-defined automated mechanisms*].

b. Take the following actions when unauthorized or misconfigured components are detected: [*Selection (one or more): disable network access by such components; isolate the components; notify* [*Assignment: organization-defined personnel or roles*]].

DISCUSSION

Monitoring for unauthorized or misconfigured system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms may also be used to prevent the connection of unauthorized or misconfigured system components. Automated mechanisms can be implemented in systems or in separate system components. When acquiring and implementing automated mechanisms, organizations consider whether such mechanisms depend on the ability of the system component to support an agent or supplicant in order to be detected since some types of components do not have or cannot support agents (e.g., IoT devices, sensors). Isolation can be achieved, for example, by placing unauthorized system components in separate domains or subnets or quarantining such components. This type of component isolation is commonly referred to as "sandboxing." This requirement enhances SP 800-171 requirement 03.04.10.

PROTECTION STRATEGY

PRA, DLO

ADVERSARY EFFECTS

Preclude (Expunge, Preempt); Impede (Contain); Expose (Detect)

REFERENCES

Source Control: CM-08(03)

03.04.03E Automation Support for System Component Inventory

Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [*Assignment: organization-defined automated mechanisms*].

DISCUSSION

The system component inventory includes system-specific information required for component accountability and to provide support to identify, control, monitor, and verify configuration items based on the authoritative source. The information necessary for the accountability of system components includes the system name, hardware and software component owners, hardware inventory specifications, software license information, software version numbers, and—for networked components—the machine names and network addresses. Inventory specifications include the manufacturer, supplier information, component type, date of receipt, cost, model, serial number, and physical location. Organizations also use automated mechanisms to implement and maintain authoritative (i.e., up-to-date, complete, accurate, and available) baseline configurations for systems that include hardware and software inventory tools, configuration management tools, and network management tools. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels. This requirement enhances SP 800-171 requirement 03.04.10.

PROTECTION STRATEGY

PRA, DLO

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Expose (Detect)

REFERENCES

Source Control: CM-08(02)

03.04.04E Automation Support for Baseline Configuration

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [*Assignment: organization-defined automated mechanisms*].

DISCUSSION

Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools; hardware, software, and firmware inventory tools; and network management tools. Automated tools can be used to track version numbers on operating systems,

applications, the types of software installed, and current patch levels. Automation support for accuracy and currency can be satisfied by the implementation of 03.04.03E for organizations that combine system component inventory and baseline configuration activities. This requirement enhances SP 800-171 requirement 03.04.01.

PROTECTION STRATEGY

PRA, DLO

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Expose (Detect)

REFERENCES

Source Control: CM-02(02)

03.04.05E Dual Authorization for System Changes

Enforce dual authorization for implementing changes to [*Assignment: organization-defined system components and system-level information*].

DISCUSSION

Dual authorization is also known as two-person control. Organizations employ dual authorization to help ensure that any changes to selected system components and system-level information cannot occur unless two qualified individuals approve and implement such changes. Requiring two individuals to implement system changes provides an increased level of assurance that the individuals carrying out those actions possess the knowledge, skills, and expertise to determine whether the proposed changes are correct implementations of approved changes. The individuals are also accountable for the changes that have been implemented. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. System-level information includes operational procedures. This requirement enhances SP 800-171 requirement 03.04.05.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: CM-5(04)

03.04.06E Retention of Previous Configurations

Retain [*Assignment: organization-defined number*] previous versions of baseline configurations of the system to support rollback.

DISCUSSION

Retaining previous versions of baseline configurations to support rollback includes hardware, software, and firmware configuration files, configuration records, and associated documentation. This requirement enhances SP 800-171 requirement 03.04.01.

PROTECTION STRATEGY

PRA, CRS

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Limit (Shorten, Reduce)

REFERENCES

Source Control: CM-02(03)

03.04.07E Testing, Validation, and Documentation of Changes

Test, validate, and document changes to the system before finalizing the implementation of the changes.

DISCUSSION

Changes to systems include modifications to hardware, software, or firmware components and defined configuration settings. Organizations ensure that testing does not interfere with system operations that support organizational missions and business functions. Individuals or groups that conduct the tests understand the system security policies and procedures associated with the specific facilities or processes. Operational systems may need to be taken offline or replicated to the extent feasible before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating protection measures. This requirement enhances SP 800-171 requirement 03.04.03.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: CM-03(02)

3.5. Identification and Authentication

03.05.01E Cryptographic Bidirectional Authentication

Authenticate [*Assignment: organization-defined devices and/or types of devices*] before establishing a system connection using bidirectional authentication that is cryptographically based.

DISCUSSION

Bidirectional authentication provides stronger protection to validate the identity of other devices for connections that are of greater risk. The requirement applies to client-server authentication, server-server authentication, and device authentication (including mobile devices). The cryptographic key for authentication transactions is stored in secure storage that is available to the authenticator application (e.g., keychain storage, Trusted Platform Module (TPM), Trusted Execution Environment (TEE), or secure element). This requirement enhances SP 800-171 requirement 03.05.02.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt, Negate), Expose (Detect)

REFERENCES

Source Controls: IA-03(01)

03.05.02E Password Managers

Use [*Assignment: organization-defined password managers*] to generate and manage passwords.

DISCUSSION

For systems in which static passwords are employed, organizations ensure that the passwords are suitably complex and that the same passwords are not employed on multiple systems. A password manager automatically generates and stores strong

and different passwords for various accounts. A potential risk of using password managers is that adversaries can target the collection of passwords generated by the password manager. Therefore, the passwords require strong protection, including encrypting the passwords and storing the collection of passwords offline in a token. This requirement enhances SP 800-171 requirement 03.05.07.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Delay, Exert)

REFERENCES

Source Control: IA-05(18)

03.05.03E Device Attestation

Implement device identification and authentication based on attestation by [*Assignment: organization-defined configuration management process*].

DISCUSSION

Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. Attestation is used to enforce a comply-to-connect policy, which prohibits system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile. Attestation can be determined via a cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the patches and updates are done securely and do not disrupt identification and authentication to other devices. This requirement enhances SP 800-171 requirement 03.05.02.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: IA-03(04)

03.05.04E Embedded Unencrypted Static Authenticators

Prohibit the use of embedded unencrypted static authenticators in applications or other forms of static storage.

DISCUSSION

In addition to applications, other forms of static storage include access scripts and function keys. Organizations exercise caution when determining whether embedded or stored authenticators are encrypted or unencrypted. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This requirement enhances SP 800-171 requirement 03.05.07.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: IA-05(07)

03.05.05E Expiration of Cached Authenticators

Prohibit the use of cached authenticators after [*Assignment: organization-defined time period*].

DISCUSSION

Cached authenticators are used to authenticate to a local machine when the network is not available. If cached authentication information is out of date, the validity of the authentication information may be questionable. This requirement enhances SP 800-171 requirement 03.05.07.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: IA-05(13)

03.05.06E Identity Proofing

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines.

b. Resolve user identities to a unique individual.

c. Collect, validate, and verify identity evidence.

DISCUSSION

Identity proofing is the process of collecting, validating, and verifying user identity information to establish credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts. Organizations may be subject to laws, Executive Orders, directives, regulations, or policies that address the collection of identity evidence.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: IA-12

3.6. Incident Response

03.06.01E Security Operations Center

Establish and maintain a security operations center.

DISCUSSION

A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to security incidents in a timely manner. The SOC is staffed with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers) and implements a combination of technical, management, and operational controls (including monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to threat and security-relevant event data from multiple sources. These sources include perimeter defenses, network devices (e.g., routers, switches), and endpoint agent data feeds. The SOC provides a holistic situational

awareness capability to help organizations determine the security posture of the system and organization. An SOC capability can be obtained in a variety of ways. Larger organizations may implement a dedicated SOC, while smaller organizations may employ third-party organizations to provide such a capability. This requirement enhances SP 800-171 requirement 03.06.01.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Limit (Shorten, Reduce); Expose (Detect)

REFERENCES

Source Control: IR-4(14)

03.06.02E Integrated Incident Response Team

Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [*Assignment: organization-defined time period*].

DISCUSSION

An integrated incident response team is a group of individuals who assess, document, and respond to incidents so that organizational systems and networks can recover quickly and implement the necessary controls to avoid future incidents. Incident response team personnel include forensic and malicious code analysts, systems security engineers, tool developers, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions.

An integrated incident response team facilitates information sharing and allows organizational personnel (e.g., developers, implementers, and operators) to leverage team knowledge of the threat and implement defensive measures that enable organizations to deter intrusions more effectively. Moreover, integrated teams promote the rapid detection of intrusions, the development of appropriate mitigations, and the deployment of effective defensive measures. Integrated incident response teams are better able to identify adversary tactics, techniques, and procedures (TTP) that are linked to the operations tempo or specific mission and business functions and to define responsive actions in a way that does not disrupt those mission and business functions. Incident response teams can be distributed within organizations to make the capability resilient. For some organizations, the incident response team can be a cross-organizational entity. This requirement enhances SP 800-171 requirement 03.06.01.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Preclude (Expunge), Impede (Contain, Exert), Limit (Shorten, Reduce), Expose (Scrutinize)

REFERENCES

Source Control: IR-4(11)

03.06.03E Behavior Analysis

Analyze anomalous or suspected adversarial behavior in or related to [*Assignment: organization-defined environments or resources*].

DISCUSSION

If the organization maintains a deception environment, an analysis of behaviors in that environment, including resources targeted by the adversary and the timing of the incident or event, can provide significant insights into adversarial TTPs. External to a deception environment, the analysis of anomalous adversarial behavior (e.g., changes in system performance or usage patterns) or suspected behavior (e.g., changes in searches for the location of specific resources) can give the organization such insight. This requirement enhances SP 800-171 requirement 03.06.01.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Expose (Detect, Reveal)

REFERENCES

Source Control: IR-04(13)

03.06.04E Automation Support for Incident Reporting

Track incidents, and collect and analyze incident information using [*Assignment: organization-defined automated mechanisms*].

DISCUSSION

Automated mechanisms for tracking incidents and collecting and analyzing incident information include Computer Incident Response Centers or other electronic

databases of incidents and network monitoring devices. This requirement enhances SP 800-171 requirement 03.06.02.

PROTECTION STRATEGY

PRA, DLO

ADVERSARY EFFECTS

Expose (Detect, Reveal)

REFERENCES

Source Control: IR-05(01)

3.7. Maintenance

03.07.01E Maintenance Tool Software Updates and Patches

Inspect maintenance tools to ensure the latest software updates and patches are installed.

DISCUSSION

Maintenance tools using outdated and/or unpatched software can provide a threat vector for adversaries and result in a significant vulnerability for organizations. This requirement enhances SP 800-171 requirement 03.07.04.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt)

REFERENCES

Source Control: MA-03(06)

3.8. Media Protection

03.08.01E Dual Authorization for Media Sanitization

Enforce dual authorization for the sanitization of [*Assignment: organization-defined system media containing CUI*].

DISCUSSION

Dual authorization is also known as two-person control. Dual authorization reduces risk related to insider threats, including adversaries who have obtained credentials. Organizations employ dual authorization to help ensure that the sanitization of system media cannot occur unless two technically qualified individuals conduct the designated task. Individuals who sanitize system media possess sufficient skills and expertise to determine whether the proposed sanitization reflects applicable federal and organizational standards, policies, and procedures. Dual authorization also helps to ensure that sanitization occurs as intended to protect against errors and false claims of having performed the sanitization actions. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. Organizations consider the risks associated with implementing dual authorization when immediate responses are necessary to help ensure public and environmental safety. This requirement enhances SP 800-171 requirement 03.08.03.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: MP-06(07)

03.08.02E Dual Authorization for System Backup Deletion and Destruction

Enforce dual authorization for the deletion or destruction of [*Assignment: organization-defined system backup information*].

DISCUSSION

Dual authorization is also known as two-person control. Dual authorization reduces risk related to insider threats, including adversaries who have obtained credentials. Dual authorization ensures that the deletion or destruction of backup information cannot occur unless two qualified individuals carry out the task. Individuals who delete or destroy backup information possess the knowledge, skills, or expertise to determine whether the proposed deletion or destruction of such information reflects organizational policies and procedures. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. Organizations also consider the risk associated with implementing dual authorization when immediate responses are necessary to ensure public and environmental safety. This requirement enhances SP 800-171 requirement 03.08.09.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: CP-09(07)

03.08.03E Testing System Backups for Reliability and Integrity

Test backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.

DISCUSSION

Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components in which the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of these aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance. This requirement enhances SP 800-171 requirement 03.08.09.

PROTECTION STRATEGY

PRA, CRS

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Limit (Shorten, Reduce)

REFERENCES

Source Control: CP-09(01)

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

a. Develop and document access agreements for systems processing, storing, or transmitting CUI.

b. Review and update the access agreements [*Assignment: organization-defined frequency*].

c. Verify that individuals requiring access to CUI and systems processing, storing, or transmitting CUI:

   1. Sign appropriate access agreements prior to being granted access; and

   2. Re-sign access agreements to maintain access to systems when access agreements have been updated or [*Assignment: organization-defined frequency*].

DISCUSSION

Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with systems processing, storing, or transmitting CUI to which they have authorized access.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt)

REFERENCES

Source Control: PS-06

03.09.04E Citizenship Requirements

Verify that individuals accessing a system processing, storing, or transmitting CUI are U.S. citizens.

DISCUSSION

Organizations may determine that individuals who need access to CUI associated with a high value asset or critical program require U.S. citizenship status. This requirement enhances SP 800-171 requirement 03.09.01.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt)

REFERENCES

Source Control: PS-03(04)

3.10. Physical Protection

03.10.01E Visitor Access Records

a. Maintain visitor access records to the facility where the system resides for [*Assignment: organization-defined time period*].

b. Review visitor access records [*Assignment: organization-defined frequency*].

c. Report anomalies in visitor access records to [*Assignment: organization-defined personnel*].

DISCUSSION

Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine whether access authorizations are current and still required to support organizational mission and business functions. Access records are not required for publicly accessible areas.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt)

REFERENCES

Source Control: PE-08

03.10.02E Intrusion Alarms and Surveillance Equipment

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

DISCUSSION

Physical intrusion alarms can be used to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and facility security guards by triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, including motion sensors, contact sensors, and broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility. This requirement enhances SP 800-171 requirement 03.10.02.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Expose (Detect, Reveal)

REFERENCES

Source Control: PE-06(01)

03.10.03E Delivery and Removal of System Components

a. Authorize and control [*Assignment: organization-defined types of system components*] entering and exiting the facility.

b. Maintain records of the system components.

DISCUSSION

Enforcing authorizations for the entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt)

REFERENCES

Source Control: PE-16

3.11. Risk Assessment

03.11.01E Threat Awareness Program

Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

DISCUSSION

Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it may be likely that adversaries can successfully breach or compromise organizational systems. One of the techniques that organizations can use to address this concern is to share threat information, including threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found to be effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats). Threat information sharing may be bilateral or multilateral. Bilateral threat sharing can include government-to-commercial and government-to-government cooperatives. Multilateral threat sharing can include organizations taking part in threat-sharing consortia. Threat information may require special agreements and protection, or it may be freely shared.

To maximize the effectiveness of monitoring and sharing threat intelligence information, it is important to know what threat observables and indicators the sensors need to be searching for. By using well-established frameworks, services, and automated tools, organizations improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Preclude (Negate), Impede (Exert), Expose (Detect)

REFERENCES

Source Controls: PM-16

03.11.02E Threat Hunting

a. Establish and maintain a cyber threat hunting capability to:

1. Search for indicators of compromise in organizational systems and
2. Detect, track, and disrupt threats that evade existing controls.

b. Implement the threat hunting capability [*Assignment: organization-defined frequency*].

DISCUSSION

Threat hunting is an active means of cyber defense in contrast to traditional protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and SIEM technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of responses. Indications of compromise include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams leverage existing threat intelligence and may create new threat intelligence that is shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies. This requirement is related to 03.11.09.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Preclude (Expunge), Limit (Shorten, Reduce), Expose (Detect, Scrutinize)

REFERENCES

Source Control: RA-10

03.11.03E Predictive Cyber Analytics

Implement the following advanced automation and analytics capabilities to predict and identify risks to [*Assignment: organization-defined systems or system components*]: [*Assignment: organization-defined advanced automation and analytics capabilities*].

DISCUSSION

A properly resourced security operations center (SOC) or computer incident response team (CIRT) may be overwhelmed by the volume of information generated by the proliferation of security tools and appliances unless it employs advanced automation and analytics to analyze the data. Advanced automation and predictive analytics capabilities are typically supported by artificial intelligence concepts and

machine learning. Examples include automated workflow operations; automated threat discovery and response, including broad-based collection, context-based analysis, and adaptive response capabilities; and machine-assisted decision tools. However, sophisticated adversaries may be able to extract information related to analytic parameters and retrain the machine learning to classify malicious activity as benign. Accordingly, machine learning is augmented by human monitoring to ensure that sophisticated adversaries are not able to conceal their activities. This requirement enhances SP 800-171 requirement 03.11.01.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Preclude (Expunge), Limit (Shorten, Reduce), Expose (Detect, Scrutinize)

REFERENCES

Source Control: RA-03(04)

03.11.04E Withdrawn

Addressed by 03.15.01E, 03.15.02.

03.11.05E Withdrawn

Addressed by 03.11.01E, 03.11.01, and 03.12.01.

03.11.06E Withdrawn

Addressed by 03.12.03E, 03.17.03E, 03.11.01, and 03.11.04.

03.11.07E Withdrawn

Addressed by 03.17.01.

03.11.08E Dynamic Threat Awareness

Determine the current cyber threat environment on an ongoing basis using [*Assignment: organization-defined means*].

DISCUSSION

The threat awareness information that is gathered feeds into the organization's security operations to ensure that procedures are updated in response to the changing threat environment. For example, at higher threat levels, organizations

may change the privilege or authentication thresholds required to perform certain operations. This requirement enhances SP 800-171 requirement 03.11.01.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Expose (Detect, Reveal)

REFERENCES

Source Control: RA-03(03)

03.11.09E Indicators of Compromise

Discover, collect, and distribute to [*Assignment: organization-defined personnel or roles*], indicators of compromise provided by [*Assignment: organization-defined sources*].

DISCUSSION

Indicators of compromise (IOCs) are forensic artifacts from intrusions that are identified on organizational systems at the host or network level. IOCs provide valuable information on systems that have been compromised. IOCs can include the creation of registry key values. IOCs for network traffic include universal resource locator (URL) or protocol elements that indicate malicious code command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that systems and organizations are vulnerable to the same exploit or attack. Threat indicators, signatures, TTPs, and other IOCs may be available via government and non-government cooperatives, including the Forum of Incident Response and Security Teams (FIRST), the Computer Emergency Response Team (CERT) Coordination Center (CERTCC), the United States Computer Emergency Readiness Team, and the Defense Industrial Base (DIB) Cybersecurity Information Sharing Program. This requirement enhances SP 800-171 requirement 03.14.06. It is also related to 03.11.02.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Expose (Detect, Reveal)

REFERENCES

Source Control: SI-04(24)

03.11.10E Criticality Analysis

Identify critical system components and functions by performing a criticality analysis for [*Assignment: organization-defined systems, system components, or system services*] at [*Assignment: organization-defined decision points in the system development life cycle*].

DISCUSSION

Not all system components, functions, or services necessarily require significant protection. For example, criticality analysis is a key tenet of risk management and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, Executive Orders, regulations, directives, policies, standards, system functionality requirements, as well as system and system component interfaces and dependencies. Organizations conduct a functional decomposition of a system to identify mission-critical functions and system components. The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities that such components create. Function and component criticality are assessed in terms of the impact of a function or component failure on the organizational missions that are supported by the system that contains the functions and components.

Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early and throughout the system development life cycle, organizations may be able to modify the system design to reduce the critical nature of these functions and components, such as by adding redundancy or alternate paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is an important consideration.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt)

REFERENCES

Source Control: RA-09

03.11.11E Discoverable Information

Determine information about the system that is discoverable and take [*Assignment: organization-defined corrective actions*].

DISCUSSION

Discoverable information includes information that adversaries could obtain without compromising or breaching the system, such as by collecting information that the system is exposing or by conducting extensive web searches. Corrective actions include notifying organizational personnel, removing designated information, or changing the system to make the designated information less relevant or attractive to adversaries. This requirement excludes intentionally discoverable information that may be part of a decoy capability (e.g., honeypots, honeynets, or deception nets) implemented by the organization. This requirement enhances SP 800-171 requirement 03.11.02.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Expose (Reveal)

REFERENCES

Source Control: RA-05(04)

03.11.12E Automated Means for Sharing Threat Intelligence

Implement automated mechanisms to maximize the effectiveness of sharing threat intelligence information.

DISCUSSION

To maximize the effectiveness of monitoring and sharing threat intelligence information, it is important to know what threat observables and indicators the sensors need to be searching for. By using well-established frameworks, services, and automated tools, organizations improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Preclude (Negate), Impede (Exert), Expose (Detect)

REFERENCES

Source Controls: PM-16(01)

3.12. Security Assessment and Monitoring

03.12.01E Penetration Testing

Conduct penetration testing [*Assignment: organization-defined frequency*] on [*Assignment: organization-defined systems or system components*].

DISCUSSION

Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning. It is conducted by penetration testing agents and teams with particular skills and experience that include technical expertise in network, operating system, and application-level security. Penetration testing can be used to validate vulnerabilities or determine a system's penetration resistance to adversaries within specified constraints, such as time, resources, and skills. Organizations may also supplement penetration testing with red team exercises. Red teams attempt to duplicate the actions of adversaries in carrying out attacks against organizations and provide an in-depth analysis of security-related weaknesses or deficiencies.

Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes pretest analysis based on full knowledge of the system, pretest identification of potential vulnerabilities based on the pretest analysis, and testing designed to determine the exploitability of vulnerabilities. All parties agree to the specified rules of engagement before the commencement of penetration testing. Organizations correlate the rules of engagement for penetration tests and red teaming exercises (if used) with the tools, techniques, and procedures that they anticipate adversaries may employ. The penetration testing or red team exercises may be organization-based or external to the organization. In either case, it is important that the team possesses the necessary skills and resources to do the job and is objective in its assessment.

PROTECTION STRATEGY

PRA, DLO

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Expose (Detect)

REFERENCES

Source Control: CA-08

03.12.02E Independent Assessors

Use independent assessors or assessment teams to conduct security requirement assessments.

DISCUSSION

Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the systems under assessment or the determination of security requirement effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments can be obtained from elements within organizations or be contracted to entities outside of organizations. Organizational officials determine the required level of independence based on the risk to organizational operations, organizational assets, or individuals. Organizational officials also determine whether the level of assessor independence provides sufficient assurance such that the assessment results are sound and can be used to make effective risk-based decisions. Independence determination includes whether contracted assessment services have sufficient independence, such as when system owners are not directly involved in the contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, having independent assessors is analogous to having independent subject-matter experts involved in design reviews.

When the structures of the organizations require that assessments be conducted by individuals that are in the developmental, operational, or management chain of the system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams

of experts to validate the completeness, accuracy, integrity, and reliability of the results. This requirement enhances SP 800-171 requirement 03.12.01.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt)

REFERENCES

Source Control: CA-02(01)

03.12.03E Risk Monitoring

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes effectiveness monitoring, compliance monitoring, change monitoring.

DISCUSSION

Risk monitoring is guided and informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security risk. This requirement enhances SP 800-171 requirement 03.12.03.

PROTECTION STRATEGY

PRA, DLO

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Expose (Detect)

REFERENCES

Source Control: CA-07(04)

03.12.04E Internal System Connections

a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system.

b. Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

c. Terminate internal system connections after [Assignment: organization-defined conditions].

d. Review [Assignment: organization-defined frequency] the continued need for each internal connection.

DISCUSSION

Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system), including components that are used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers. For efficiency, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: CA-09

3.13. System and Communications Protection

03.13.01E Heterogeneity

Use a diverse set of information technologies for the following system components in the implementation of the system: [*Assignment: organization-defined system components*].

DISCUSSION

Increasing the diversity of information technologies within organizational systems reduces the impact of exploitations or compromises of specific technologies. Such diversity protects against common mode failures, including those induced by supply chain attacks. Diversity in information technologies reduces the likelihood that the means adversaries use to compromise one system component will be effective

against other system components, further increasing the adversary work factor to successfully complete planned attacks. An increase in diversity may add complexity and management overhead that could ultimately lead to mistakes and unauthorized configurations.

PROTECTION STRATEGY

PRA, CRS

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Contain, Exert), Limit (Reduce)

REFERENCES

Source Control: SC-29

03.13.02E Randomness

Use the following techniques to introduce randomness into organizational operations and assets: [*Assignment: organization-defined techniques*].

DISCUSSION

Randomness introduces increased levels of uncertainty for adversaries regarding the actions that organizations take to defend their systems against attacks. Such actions may impede the ability of adversaries to correctly target organizational systems that support critical missions or business functions. Uncertainty may cause adversaries to hesitate before initiating or continuing attacks. Misdirection techniques that involve randomness include performing certain routine actions at different times of day, employing different information technologies, using different suppliers, and rotating the roles and responsibilities of organizational personnel.

PROTECTION STRATEGY

PRA, CRS

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Redirect (Deceive)

REFERENCES

Source Control: SC-30(02)

03.13.03E Concealment and Misdirection

Use the following concealment and misdirection techniques to confuse and mislead adversaries: [*Assignment: organization-defined concealment and misdirection techniques*].

DISCUSSION

Concealment and misdirection techniques can significantly reduce the targeting capabilities of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete attacks. For example, virtualization techniques provide organizations with the ability to disguise systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. The increased use of specific concealment and misdirection techniques and methods, including randomness, uncertainty, and virtualization, may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery or exposing tradecraft. Concealment and misdirection techniques may provide additional time to perform core mission and business functions. The implementation of concealment and misdirection techniques may add to the complexity and management overhead required for the system.

PROTECTION STRATEGY

PRA, CRS

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Redirect (Deceive)

REFERENCES

Source Control: SC-30

03.13.04E Isolation of System Components

Implement boundary protection mechanisms to isolate [*Assignment: organization-defined system components*].

DISCUSSION

Organizations can isolate system components that perform different mission or business functions. Isolating system components with boundary protection mechanisms allows for the increased protection of individual system components and more effective control of information flows between those components. Isolating system components provides enhanced protection that limits the potential harm of hostile cyber-attacks and errors. The degree of isolation varies depending on the mechanisms selected. Boundary protection mechanisms include routers, gateways, and firewalls that separate system components into physically separate

networks or subnetworks; cross-domain devices that separate subnetworks; virtualization techniques; and the encryption of information flows among system components using distinct encryption keys. This requirement enhances SP 800-171 requirement 03.13.01.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Limit (Reduce)

REFERENCES

Source Control: SC-07(21)

03.13.05E Change Processing and Storage Locations

Change the location of [*Assignment: organization-defined processing and/or storage*] [*Selection (one):* [*Assignment: organization-defined time frequency*]*; at random time intervals*].

DISCUSSION

Adversaries target critical missions and business functions and the systems that support those missions and business functions while also trying to minimize the exposure of their existence and tradecraft. The homogeneous, deterministic, and static nature of organizational systems targeted by adversaries make such systems more susceptible to attacks with less adversary cost and effort to be successful. Changing processing and storage locations (also referred to as moving target defense) addresses the advanced persistent threat using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the system components (i.e., processing, storage) that support critical missions and business functions. Changing the locations of processing activities and/or storage sites introduces a degree of uncertainty to the targeting activities of adversaries. The targeting uncertainty increases the work factor of adversaries and makes compromises or breaches of the organizational systems more difficult and time-consuming. Uncertainty also increases the chances that adversaries may inadvertently disclose certain aspects of their tradecraft while attempting to locate critical organizational assets.

PROTECTION STRATEGY

CRS

ADVERSARY EFFECTS

Preclude (Preempt, Negate), Impede (Contain, Exert), Limit (Reduce)

REFERENCES

Source Control: SC-30(3)

03.13.06E Platform-Independent Applications

Implement the following platform-independent applications within organizational systems: [*Assignment: organization-defined platform-independent applications*].

DISCUSSION

Platforms are the hardware, software, and firmware components used to execute the organization's software applications. Platforms include operating systems, the underlying computer architectures, or both. Platform-independent applications are applications with the capability to execute on multiple platforms. Such applications promote portability and reconstitution on different platforms. The portability of applications and the ability to reconstitute applications on different platforms increase the availability of mission-essential functions within organizations when systems with specific operating systems are under attack.

PROTECTION STRATEGY

CRS

ADVERSARY EFFECTS

Limit (Shorten, Reduce)

REFERENCES

Source Control: SC-27

03.13.07E Virtualization Techniques

Use virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [*Assignment: organization-defined frequency*].

DISCUSSION

While frequent changes to operating systems and applications can pose significant configuration management challenges, the changes can result in an increased work factor for adversaries to conduct successful attacks. Changing virtual operating systems or applications, as opposed to changing actual operating systems or applications, provides virtual changes that impede attacker success while reducing

configuration management efforts. Virtualization techniques can assist in isolating untrustworthy software or software of dubious provenance into confined execution environments.

PROTECTION STRATEGY

PRA, CRS

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Limit (Reduce)

REFERENCES

Source Control: SC-29(01)

03.13.08E Decoys

Use components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.

DISCUSSION

Decoys (i.e., honeypots, honeynets, or deception nets) are established to attract adversaries and deflect attacks away from the operational systems that support organizational missions and business functions. The use of decoys requires some supporting isolation measures to ensure that any deflected malicious code does not infect organizational systems.

PROTECTION STRATEGY

DLO, CRS

ADVERSARY EFFECTS

Expose (Detect), Limit (Reduce)

REFERENCES

Source Control: SC-26

03.13.09E Security Tool, Mechanism, and Support Component Isolation

Isolate [*Assignment: organization-defined information security tools, mechanisms, and support components*] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

DISCUSSION

Physically separate subnetworks with managed interfaces are useful for isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques employed by organizations. This requirement enhances SP 800-171 requirement 03.13.01.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: SC-07(13)

03.13.10E Separate Subnetworks

Implement separate network addresses to connect to systems in different security domains.

DISCUSSION

The decomposition of systems into subnetworks (i.e., subnets) helps to provide the appropriate level of protection for network connections to security domains that contain information with different sensitivity levels. This requirement enhances SP 800-171 requirement 03.13.01.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Limit (Reduce)

REFERENCES

Source Control: SC-07(22)

03.13.11E Thin Nodes

Implement minimal functionality and information storage on the following system components: [*Assignment: organization-defined system components*].

DISCUSSION

The deployment of system components with minimal functionality reduces the need to secure every endpoint and may reduce the exposure of information, systems, and services to attacks. Reduced or minimal functionality includes diskless nodes and thin client technologies.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Contain)

REFERENCES

Source Control: SC-25

03.13.12E Denial-of-Service Protection

a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events].

b. Implement the following safeguards to achieve the denial-of-service [Assignment: organization-defined safeguards by type of denial-of-service event].

DISCUSSION

Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Cyber-attacks can occur across a wide range of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events.

PROTECTION STRATEGY

PRA, CRS

ADVERSARY EFFECTS

Preclude (Preempt, Negate), Impede (Exert), Limit (Reduce)

REFERENCES

Source Control: SC-05

03.13.13E Port and Input/Output Device Access

[*Selection (one): Physically; Logically*] disable or remove [*Assignment: organization-defined connection ports or input/output devices*] on the following systems or system components: [*Assignment: organization-defined systems or system components*].

DISCUSSION

Connection ports include Universal Serial Bus (USB), Thunderbolt, and Firewire (IEEE 1394). Input/output (I/O) devices include compact disc and digital versatile disc drives. Disabling or removing such connection ports and I/O devices helps prevent the exfiltration of information from systems and the introduction of malicious code from those ports or devices. Physically disabling or removing ports and/or devices is the stronger action.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Contain)

REFERENCES

Source Control: SC-41

03.13.14E Detonation Chambers

Implement a detonation chamber capability within [*Assignment: organization-defined system, system component, or location*].

DISCUSSION

Detonation chambers (also known as dynamic execution environments) allow organizations to open email attachments, execute untrusted or suspicious applications, and execute URL requests in the safety of an isolated environment or a virtualized sandbox. Protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code. While related to the concept of deception nets, the employment of detonation chambers is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, detonation chambers are intended to quickly identify malicious code and reduce the likelihood

that the code is propagated to user environments of operation or prevent such propagation completely.

PROTECTION STRATEGY

PRA, DLO

ADVERSARY EFFECTS

Preclude (Preempt), Negate), Impede (Contain, Exert), Expose (Detect, Reveal)

REFERENCES

Source Control: SC-44

3.14. System and Information Integrity

03.14.01E Software, Firmware, and Information Integrity

a. Use integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [*Assignment: organization-defined software, firmware, and information*].

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [*Assignment: organization-defined actions*].

DISCUSSION

Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes boot firmware, operating systems with key internal components (e.g., kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output Systems (BIOS). Information includes CUI and metadata that contains security attributes associated with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

Verifying the integrity of the organization's security-critical or essential software is an important capability since corrupted software is the primary attack vector used by adversaries to undermine or disrupt the proper functioning of organizational systems. This capability helps system components protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of updates to the firmware prior to applying changes to the system component and preventing unauthorized processes from modifying the boot firmware. There are many ways to verify software integrity throughout the system development life

cycle. Root of trust mechanisms (e.g., secure boot, trusted platform modules, UEFI) verify that only trusted code is executed during boot processes. The employment of cryptographic signatures ensures the integrity and authenticity of critical software that stores, processes, or transmits, CUI. Cryptographic signatures include digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Hardware roots of trust are considered to be more secure.

PROTECTION STRATEGY

PRA, DLO

ADVERSARY EFFECTS

Preclude (Preempt), Expose (Detect)

REFERENCES

Source Control: SI-07

03.14.02E Withdrawn

Addressed by 03.14.06.

03.14.03E Withdrawn

Addressed by 03.15.01E, 03.13.01, and 03.16.01.

03.14.04E Refresh from Trusted Sources

Obtain software and data employed during system component and service refreshes from the following trusted sources: [*Assignment: organization-defined trusted sources*].

DISCUSSION

Trusted sources include software and data from write-once, read-only media or from selected offline secure storage facilities.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: SI-14(01)

03.14.05E Non-Persistent Information

a. [*Selection (one): Refresh* [*Assignment: organization-defined information*] [*Assignment: organization-defined frequency*]*; Generate* [*Assignment: organization-defined information*] *on demand*].

b. Delete information when no longer needed.

DISCUSSION

Retaining unneeded information makes that information a potential target for advanced adversaries searching for high value assets to compromise through unauthorized disclosure, unauthorized modification, or exfiltration. For system-related information, unnecessary retention provides advanced adversaries information that can assist in their reconnaissance and lateral movement through the system.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: 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, 03.16.01.

03.14.08E Integrity Checks

Perform an integrity check of [*Assignment: organization-defined software, firmware, and information*] [*Selection (one or more): at startup; at* [*Assignment: organization-defined transitional states or security-relevant events*]; [*Assignment: organization-defined frequency*]].

DISCUSSION

Security-relevant events include the identification of new threats to which systems are susceptible and the installation of hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: SI-07(01)

03.14.09E Cryptographic Protection

Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

DISCUSSION

Cryptographic mechanisms used to protect integrity include digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Organizations that employ cryptographic mechanisms also consider cryptographic key management solutions.

PROTECTION STRATEGY

PRA, DLO

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Expose (Detect)

REFERENCES

Source Control: SI-07(06)

03.14.10E Protection of Boot Firmware

Implement the following mechanisms to protect the integrity of boot firmware in [*Assignment: organization-defined system components*]: [*Assignment: organization-defined mechanisms*].

DISCUSSION

Unauthorized modifications to boot firmware may indicate a sophisticated, targeted attack. These types of targeted attacks can result in a permanent denial of service or a persistent malicious code presence. These situations can occur if the firmware is corrupted or if the malicious code is embedded within the firmware. System components can protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of updates to the firmware prior to applying changes to the system component and preventing unauthorized processes from modifying the boot firmware.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: SI-07(10)

03.14.11E Integration of Detection and Response Capability

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [*Assignment: organization-defined security-relevant changes to the system*].

DISCUSSION

Integrating a detection and response capability ensures that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Expose (Detect)

REFERENCES

Source Control: SI-07(07)

03.14.12E Information Input Validation

Check the validity of the following information inputs: [*Assignment: organization-defined information inputs to the system*].

DISCUSSION

Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of "387," "abc," or "%K%" are invalid and not accepted as inputs to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components.

Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks, such as cross-site scripting and a variety of injection attacks.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt)

REFERENCES

Source Control: SI-10

03.14.13E Error Handling

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

b. Reveal error messages only to [*Assignment: organization-defined personnel or roles*].

DISCUSSION

Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information, such as account numbers, Social Security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt)

REFERENCES

Source Control: SI-11

03.14.14E Memory Protection

Implement the following safeguards to protect the system memory from unauthorized code execution: [*Assignment: organization-defined safeguards*].

DISCUSSION

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. The safeguards used to protect memory include data execution prevention and address space layout randomization (ASLR). Data execution prevention safeguards can be hardware- or software-enforced with hardware enforcement providing the greater strength of mechanism.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: SI-16

03.14.15E Non-Persistent System Components and Services

a. Identify the following non-persistent system components and services: [*Assignment: organization-defined system components and services*].

b. Initiate non-persistent system components and services from a known state.

c. Terminate non-persistent system components and services [*Selection (one or more): upon end of session of use; at* [*Assignment: organization-defined frequency*]].

DISCUSSION

By implementing the concept of non-persistence for selected system components and services, organizations can provide a trusted computing resource for a specific time period that does not give adversaries sufficient time to exploit vulnerabilities in organizational systems and operating environments. The use of non-persistent components and services mitigates risk by limiting the targeting capability of adversaries (i.e., reducing the window of opportunity and available attack surface) to initiate and complete attacks. Since the APT is a sophisticated threat with regard to adversary capability, organizations can assume that a percentage of attacks will be successful over an extended period. Non-persistent system components and services are activated as required from a known (trusted) state and terminated periodically or at the end of sessions. The use of non-persistent system components and services also increases the work factor of adversaries.

Non-persistence can be achieved by refreshing system components, periodically reimaging components, or using a variety of common virtualization techniques. Non-persistent services can be implemented by using virtual machines or as new instances of processes on physical machines (persistent or non-persistent). The benefit of periodic refreshes of system components and services is that it does not require organizations to determine in advance whether compromises have occurred, which may be difficult or impossible. The refresh of selected system components and services occurs with sufficient frequency to prevent the spread or intended impact of attacks but not with such frequency that it makes the system unstable.

PROTECTION STRATEGY

PRA, CRS

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Limit (Shorten, Reduce)

REFERENCES

Source Control: SI-14

03.14.16E Tainting

Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: [*Assignment: organization-defined systems or system components*].

DISCUSSION

Many cyber-attacks target organizational information or information that the organization holds on behalf of other entities with the intent to exfiltrate that information. In addition, insider attacks and erroneous user procedures can remove information from the system in violation of organizational policies. Tainting approaches can range from passive to active. A passive tainting approach can be as simple as adding false email names and addresses to an internal database. If the organization receives email at one of the false email addresses, it knows that the database has been compromised. Moreover, the organization knows that the email was sent by an unauthorized entity, so any packets it includes potentially contain malicious code, and the unauthorized entity may have potentially obtained a copy of the database. Another tainting approach includes embedding false data or steganographic data in files to enable the data to be found via open-source analysis. An active tainting approach can include embedding software in the data that is able to "call home," thereby alerting the organization to its capture and possibly its location and the path by which it was exfiltrated or removed.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Expose (Detect)

REFERENCES

Source Control: SI-20

03.14.17E System-Generated Alerts

Alert [*Assignment: organization-defined personnel or roles*] when the following system-generated indications of compromise or potential compromise occur: [*Assignment: organization-defined compromise indicators*].

DISCUSSION

Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and transmitted telephonically, by electronic mail

messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners or stewards, chief information security officers, and system security officers. In contrast to alerts generated by the system, alerts generated by the organization focuses on information sources external to the system, such as suspicious activity reports and reports on potential insider threats. This requirement enhances SP 800-171 requirement 03.14.06.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Expose (Detect)

REFERENCES

Source Controls: SI-04(05)

03.14.18E Automated Organization-Generated Alerts

Alert [*Assignment: organization-defined personnel or roles*] using [*Assignment: organization-defined automated mechanisms*] when the following indications of inappropriate or unusual activities with security implications occur: [*Assignment: organization-defined activities that trigger alerts*].

DISCUSSION

The sources for organization-generated alerts are focused on entities such as suspicious activity reports and reports on potential insider threats. Organizational personnel on the system alert notification list include system administrators, mission or business owners, system owners, chief information security officers, and system security officers. In contrast to the alerts generated by the organization, alerts generated by the system focus on information sources that are internal to the system, such as audit records. This requirement enhances SP 800-171 requirement 03.14.06.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Expose (Detect)

REFERENCES

Source Controls: SI-04(12)

3.15. Planning

03.15.01E Security Architecture

a. Develop a security architecture for the system that:

   1. Describes the security requirements and approach to be taken for protecting the confidentiality, integrity, and availability of CUI,

   2. Describes how the architecture is integrated into and supports the enterprise architecture, and

   3. Describes any assumptions about, and dependencies on, external systems and services.

b. Review and update the security architecture [*Assignment: organization-defined frequency*] to reflect changes in the enterprise architecture.

c. Reflect planned security architecture changes in system security plans, concept of operations, criticality analysis, organizational procedures, and procurements and acquisitions.

DISCUSSION

The security architecture at the system level is consistent with the organization-wide security architecture, which is integral to and developed as part of the enterprise architecture. The security architecture includes an architectural description, the allocation of security functionality (i.e., safeguards and countermeasures), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The architectures can also include other information, such as user roles and the access privileges assigned to each role; security requirements; types of information processed, stored, and transmitted by the system; supply chain risk management (SCRM) requirements; restoration priorities of information and system services; and other protection needs.

With the use of modern computing technologies, it is becoming less common for organizations to control all information resources. There may be key dependencies on external services and service providers. Describing such dependencies as part of the security architecture is necessary for developing a comprehensive protection strategy. Establishing, documenting, and maintaining a baseline configuration for organizational systems under configuration control is critical to implementing and maintaining an effective security architecture. Guidance on developing trustworthy, secure, and cyber-resilient systems using systems security engineering practices and security design concepts is provided in [22].

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: PL-08

03.15.02E Defense In Depth

a. Design the security architecture for the system using a defense-in-depth approach.

b. Allocate [*Assignment: organization-defined security requirements*] to [*Assignment: organization-defined architectural layers and locations*].

c. Ensure that the allocated requirements operate in a coordinated and mutually reinforcing manner.

DISCUSSION

Organizations strategically allocate security requirements and the associated protection mechanisms in the security architecture so that adversaries must overcome multiple defensive layers to achieve their objective. Requiring adversaries to defeat multiple defensive layers makes it more difficult to attack systems by increasing the work factor of the adversary. It also increases the likelihood of detection. Defense-in-depth architectural approaches include modularity and layering, the separation of system and user functionality, and security function isolation.

The coordination of allocated security requirements is essential to help ensure that an attack that involves one requirement does not create adverse, unintended consequences (e.g., system lockout and cascading alarms) by interfering with other requirements. The value of organizational assets and the impacts or consequences of loss are important considerations in providing additional defensive layers.

PROTECTION STRATEGY

PRA, CRS

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert), Limit (Reduce)

REFERENCES

Source Control: PL-08(01)

03.15.03E Supplier Diversity

Require that [*Assignment: organization-defined safeguards*] allocated to [*Assignment: organization-defined locations and architectural layers*] are obtained from different suppliers.

DISCUSSION

Information technology security products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors that offer malicious code protection typically update their products at different times and develop solutions for known viruses, Trojans, or worms based on their priorities and development schedules. Deploying different types of products at different locations increases the likelihood that at least one of the products will detect the malicious code.

PROTECTION STRATEGY

PRA, CRS

ADVERSARY EFFECTS

Preclude (Preempt, Negate), Impede (Exert), Limit (Reduce)

REFERENCES

Source Control: PL-08(02)

3.16. System and Services Acquisition

03.16.01E Specialization

Implement [*Selection (one or more): design; modification; augmentation; reconfiguration*] on [*Assignment: organization-defined systems or system components*] supporting mission-essential services or functions to increase the trustworthiness in those systems or components.

DISCUSSION

Systems or system components that support mission-essential services or functions must often be enhanced to maximize the trustworthiness of the resource. Sometimes, this enhancement is done at the design level. In other instances, it is done post-design, either through modifications of the system in question or by augmenting the system with additional components. For example, supplemental

authentication or non-repudiation functions may be added to the system to enhance critical resources that depend on the organization-defined resources.

PROTECTION STRATEGY

PRA

ADVERSARY EFFECTS

Preclude (Preempt), Impede (Exert)

REFERENCES

Source Control: SA-23

3.17. Supply Chain Risk Management

03.17.01E Notification Agreements

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service regarding the [*Selection (one or more): notification of supply chain compromises; results of assessments or audits; provision of* [*Assignment: organization-defined information*]].

DISCUSSION

Establishing agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that may adversely affect or have adversely affected organizational systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Expose (Detect), Limit (Shorten, Reduce)

REFERENCES

Source Control: SR-08

03.17.02E Inspection of Systems or Components

Inspect the following systems or system components [*Selection (one or more): at random;* [*Assignment: organization-defined frequency*]*; upon* [*Assignment: organization-defined indications of need for inspection*]] to detect tampering: [*Assignment: organization-defined systems or system components*].

DISCUSSION

Inspecting systems or systems components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components that are removed from organization-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased and when individuals return from travel to high-risk locations.

PROTECTION STRATEGY

DLO

ADVERSARY EFFECTS

Expose (Detect)

REFERENCES

Source Control: SR-10

03.17.03E Component Authenticity

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system.

b. Report counterfeit system components to [*Selection (one or more): source of counterfeit component;* [*Assignment: organization-defined external reporting organizations*]*;* [*Assignment: organization-defined personnel or roles*]].

DISCUSSION

Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include the Cybersecurity and Infrastructure Security Agency (CISA).

PROTECTION STRATEGY

PRA, DLO

ADVERSARY EFFECTS

Preclude (Preempt), Expose (Detect)

REFERENCES

Source Control: SR-11

References

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

[2] Executive Order 13526 (2009) Classified National Security Information. (The White House, Washington, DC), DCPD-200901022, December 29, 2009. Available at https://www.govinfo.gov/app/details/DCPD-200901022

[3] Atomic Energy Act (P.L. 83-703), August 1954. Available at https://www.govinfo.gov/app/details/STATUTE-68/STATUTE-68-Pg919

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

[5] 32 CFR Part 2002 (2016), Controlled Unclassified Information (CUI), September 2016. Available at https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018-title32-vol6-part2002.pdf

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

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

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

[9] Department of Defense, Defense Acquisition University (2020), DAU Glossary of Defense Acquisition Acronyms and Terms. https://www.dau.edu/glossary/Pages/Glossary.aspx

[10] Office of Management and Budget (2018) Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program. (The White House, Washington, DC), OMB Memorandum M-19-03, December 10, 2018. Available at https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

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

[12] Ross RS, Pillitteri VY (2024) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171r3. https://doi.org/10.6028/NIST.SP.800-171r3

[13] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v2r1. https://doi.org/10.6028/NIST.SP.800-160v2r1

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

[15] Joint Task Force Transformation Initiative (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

[16] 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

[17] 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

[18] Office of Management and Budget 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

[19] U.S. Government Accountability Office (2018) Weapons Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities. (GAO, Washington, DC), Report to the Committee on Armed Services, U.S. Senate, GAO 19-128. Available at https://www.gao.gov/assets/700/694913.pdf

[20] Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed. Available at https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3552

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

[22] Ross R, Winstead M, McEvilley M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v1r1. https://doi.org/10.6028/NIST.SP.800-160v1r1

[23] Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards. 2017 ed. Available at https://www.govinfo.gov/app/details/USCODE-2017-title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331

[24] Title 44 U.S. Code, Sec. 3502, Definitions. 2017 ed. Available at https://www.govinfo.gov/app/details/USCODE-2021-title44/USCODE-2021-title44-chap35-subchapI-sec3502

[25] National Institute of Standards and Technology (2019) Roots of Trust Project. Available at https://csrc.nist.gov/projects/hardware-roots-of-trust

[26] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-128, Includes updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128

Appendix A. Acronyms

APT
Advanced Persistent Threat

ASLR
Address Space Layout Randomization

BIOS
Basic Input/Output System

CERT
Computer Emergency Response Team

CERTCC
CERT Coordination Center

CFR
Code of Federal Regulations

CIRT
Cyber Incident Response Team

CISA
Cybersecurity and Infrastructure Security Agency

CNSS
Committee on National Security Systems

CRS
Cyber Resiliency

CUI
Controlled Unclassified Information

DIB
Defense Industrial Base

DIB CS
Defense Industrial Base Cybersecurity Sharing

DLO
Damage-Limiting Operations

EO
Executive Order

FIPS
Federal Information Processing Standards

FIRST
Forum of Incident Response and Security Teams

FISMA
Federal Information Security Modernization Act

FOIA
Freedom of Information Act

GAO
Government Accountability Office

HVA
High Value Asset

IIoT
Industrial Internet of Things

IoT
Internet of Things

ISAC
Information Sharing and Analysis Centers

ISAO
Information Sharing and Analysis Organizations

ISOO
Information Security Oversight Office

IT
Information Technology

ITL
Information Technology Laboratory

NARA
National Archives and Records Administration

NIST
National Institute of Standards and Technology

NIST IR
NIST Interagency or Internal Report

ODP
Organization-Defined Parameter

OMB
Office of Management and Budget

OT
Operational Technology

PIN
Personal Identification Number

PLC
Programmable Logic Controller

PRA
Penetration-Resistant Architecture

ROI
Return on Investment

SCRM
Supply Chain Risk Management

SIEM
Security Information and Event Management

SOC
Security Operations Center

SP
Special Publication

TEE
Trusted Execution Environment

TPM
Trusted Platform Module

TTP
Tactics, Techniques, and Procedures

USC
United States Code

UEFI
Unified Extensible Firmware Interface

Appendix B. Glossary

Appendix B provides definitions for the terminology used in SP 800-172r1. The definitions are consistent with the definitions contained in the National Information Assurance Glossary [16] unless otherwise noted.

advanced persistent threat
An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period, adapts to defenders' efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives. [17]

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. [18]

assessment
See *security control assessment*.

assessor
See *security control assessor*.

attack surface
The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from that system, system element, or environment. [19]

audit record
An individual entry in an audit log related to an audited event.

authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. [7, adapted]

availability
Ensuring timely and reliable access to and use of information. [20]

baseline configuration
A documented set of specifications for a system or a configuration item within a system that has been formally reviewed and agreed on at a given point in time and which can be changed only through change control procedures.

bidirectional authentication
Two parties authenticating each other at the same time. Also known as *mutual authentication* or two-way authentication.

boundary
Physical or logical perimeter of a system.

component
See *system component*.

confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [20]

configuration management
A collection of activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

configuration settings
The set of parameters that can be changed in hardware, software, or firmware that affect the security posture or functionality of the system.

controlled unclassified information
Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. [1]

critical program (or technology)
A program which significantly increases capability, mission effectiveness, or extends the expected effective life of an essential system/capability. [1]

CUI categories
Those types of information for which laws, regulations, or government-wide policies require or permit agencies to exercise safeguarding or dissemination controls and which the CUI Executive Agent has approved and listed in the CUI Registry. [5]

CUI Executive Agent
The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees federal agency actions to comply with Executive Order 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO). [5]

CUI program
The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI Registry. [5]

cyber-physical system
Interacting digital, analog, physical, and human components engineered for function through integrated physics and logic.

cyber resiliency
The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. [13]

damage-limiting operations
Procedural and operational measures that use system capabilities to maximize the ability of an organization to detect successful system compromises by an adversary and to limit the effects of such compromises (both detected and undetected).

defense-in-depth
Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

discussion
Statements used to provide additional explanatory information for security controls or security control enhancements.

disinformation
The process of providing deliberately deceptive information to adversaries to mislead or confuse them regarding the security posture of the system or organization or the state of cyber preparedness.

dual authorization
The system of storage and handling designed to prohibit individual access to certain resources by requiring the presence and actions of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. [16, adapted]

enhanced security requirements
Security requirements that can be implemented in addition to the requirements in NIST Special Publication 800-171. The additional security requirements provide the foundation for a defense-in-depth protection strategy that includes three mutually supportive and reinforcing components: (1) penetration-resistant architecture, (2) damage-limiting operations, and (3) cyber resiliency.

executive agency
An executive department specified in 5 U.S.C. Sec. 101; a military department specified in 5 U.S.C. Sec. 102; an independent establishment as defined in 5 U.S.C. Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C. Chapter 91. [18]

external network
A network not controlled by the organization.

external system (or component)
A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

federal agency
See *executive agency*.

federal information system
An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. [23]

firmware
Computer programs and data stored in hardware—typically in read-only memory (ROM) or programmable read-only memory (PROM)—such that programs and data cannot be dynamically written or modified during execution of the programs. See *hardware* and *software*.

hardware
The material physical components of a system. See *software* and *firmware*.

high value asset
A designation of federal information or a federal information system when it relates to one or more of the following categories:

- *Informational Value*: The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries.
- *Mission-Essential*: The agency that owns the information or information system cannot accomplish its Primary Mission-Essential Functions (PMEF), as approved in accordance with Presidential Policy Directive

40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system.

- *Federal Civilian Enterprise Essential (FCEE)*: The information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise. [10]

impact
With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.

impact value
The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate, or high. [6]

incident
An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. [20]

industrial Internet of Things
The sensors, instruments, machines, and other devices that are networked together and use Internet connectivity to enhance industrial and manufacturing business processes and applications.

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. [18]

information flow control
Procedure to ensure that information transfers within a system are not made in violation of the security policy.

information resources
Information and related resources, such as personnel, equipment, funds, and information technology. [24]

information security
The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [20]

information system
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [24]

information technology
Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use. [18]

insider threat
The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.

integrity
Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [20]

Internet of Things
The network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information.

malicious code
Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

media
Physical devices or writing surfaces, including but not limited to magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system. [7]

misdirection
The process of maintaining and employing deception resources or environments and directing adversary activities to those resources or environments.

mobile device
A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-readers.

moving target defense
The concept of controlling change across multiple system dimensions in order to increase uncertainty and apparent complexity for attackers, reduce their window of opportunity, and increase the costs of their probing and attack efforts.

mutual authentication
The process of both entities involved in a transaction verifying each other. See *bidirectional authentication*.

network
A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

network access
Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

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.

on behalf of (an agency)
A situation that occurs when (i) a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting federal information; and (ii) those activities are not incidental to providing a service or product to the Government. [5]

operational technology
The hardware, software, and firmware components of a system used to detect or cause changes in physical processes through the direct control and monitoring of physical devices.

organization
An entity of any size, complexity, or positioning within an organizational structure. [7, adapted]

penetration-resistant architecture
An architecture that uses technology and procedures to limit the opportunities for an adversary to compromise an organizational system and achieve a persistent presence in the system.

personnel security
The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities requiring trustworthiness. [8]

potential impact
The loss of confidentiality, integrity, or availability could be expected to have (i) a limited adverse effect (FIPS Publication 199 low); (ii) a serious adverse effect (FIPS Publication 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals. [6]

privileged user
A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

records
The recordings (automated and manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

remote access
Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

replay resistant
Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

risk
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. [18]

risk assessment
The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation of a system. [21]

roots of trust
Highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. Roots of trust provide a firm foundation from which to build security and trust. [25]

sanitization
Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible.

security
A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach.

security assessment
See *security control assessment*.

security control
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. [18]

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. [18]

security domain
A domain that implements a security policy and is administered by a single authority. [16, adapted]

security functions
The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

security solution
The key design, architectural, and implementation choices made by organizations in satisfying specified security requirements for systems or system components.

system
See *information system*.

system component
A discrete, identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware. [26]

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

system service
A capability provided by a system that facilitates information processing, storage, or transmission.

tactics, techniques, and procedures
The behavior of an actor. A tactic is the highest-level description of the behavior; techniques provide a more detailed description of the behavior in the context of a tactic; and procedures provide a lower-level, highly detailed description of the behavior in the context of a technique. [14]

tainting
The process of embedding covert capabilities in information, systems, or system components to allow organizations to be alerted to the exfiltration of information.

threat
Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [21]

threat information
Any information related to a threat that might help an organization protect itself against the threat or detect the activities of an actor. Major types of threat information include indicators, TTPs, security alerts, threat intelligence reports, and tool configurations. [14]

threat intelligence
Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes. [14]

Appendix C. Summary of Enhanced Security Requirements

This appendix provides a consolidated list of the enhanced security requirements in Sec. 3.

Table 2. Enhanced security requirements

REQUIREMENT NUMBER	ENHANCED SECURITY REQUIREMENT
Access Control	
03.01.01E	Dual Authorization for Commands and Actions
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 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
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	Audit Record Storage in Separate Environment
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 or Misconfigured Component Detection
03.04.03E	Automation Support 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
Identification and Authentication	
03.05.01E	Cryptographic Bidirectional Authentication
03.05.02E	Password Managers
03.05.03E	Device Attestation
03.05.04E	Embedded Unencrypted Static Authenticators
03.05.05E	Expiration of Cached Authenticators
03.05.06E	Identity Proofing

REQUIREMENT NUMBER	ENHANCED SECURITY REQUIREMENT
Incident Response	
03.06.01E	Security Operations Center
03.06.02E	Integrated Incident Response Team
03.06.03E	Behavior Analysis
03.06.04E	Automation Support for Incident Reporting
Maintenance	
03.07.01E	Maintenance Tool Software Updates and Patches
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
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	Visitor Access Records
03.10.02E	Intrusion Alarms and Surveillance Equipment
03.10.03E	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
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

REQUIREMENT NUMBER	ENHANCED SECURITY REQUIREMENT
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	Security Tool, Mechanism, and Support Component 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
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
03.14.010E	Protection of Boot Firmware
03.14.11E	Integration of Detection and Response Capability
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	
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

2807

Appendix D. Adversary Effects

Cyber resiliency solutions are only relevant if they have some effect on risk, specifically by reducing the likelihood of the occurrence of threat events,[20] the ability of threat events to cause harm, and the extent of that harm.[21] The types of analysis of system architectures, designs, implementations, and operations that are indicated for cyber resiliency can include considering the effects that alternatives could have on the threat events in scenarios of concern to organizations.

From the perspective of protecting a system against adversarial threats, five high-level, desired effects on the adversary can be identified: *redirect*, *preclude*, *impede*, *limit*, and *expose*. These effects are useful for discussion but are often too general to facilitate the definition of specific measures of effectiveness. Therefore, more specific classes of effects are defined:

- *Deter*, *divert*, and *deceive* in support of **redirect**
- *Negate*, *preempt*, and *expunge* in support of **preclude**
- *Contain*, *degrade*, *delay*, and *exert* in support of **impede**
- *Shorten* and *reduce* in support of **limit**
- *Detect*, *reveal*, and *scrutinize* in support of **expose**

These effects are tactical (i.e., local to a specific threat event or scenario), although it is possible that their repeated achievement could have strategic effects as well.

Table 3 defines the effects, indicates how each effect could reduce risk, and illustrates how the use of certain approaches to implementing cyber resiliency techniques for protection against attack could have the identified effect.[22] The term "defender" refers to the organization or organizational staff responsible for providing or applying protections. It should be noted that likelihoods and impact can be reduced, but risk cannot be eliminated. Thus, no effect can be assumed to be complete, even those with names that suggest completeness, such as negate, detect, or expunge.

[20] The term "threat event" refers to an event or situation that has the potential to cause undesirable consequences or impacts. Threat events can be caused by adversarial or non-adversarial threat sources. However, this section emphasizes the effect on adversarial threats and specifically on the APT, for which threat events can be identified with adversary activities.

[21] While different risk models are valid and useful, three elements are common across most models: (1) the likelihood of occurrence (i.e., the likelihood that a threat event or a threat scenario consisting of a set of interdependent events will occur or be initiated by an adversary), (2) the likelihood of impact (i.e., the likelihood that a threat event or threat scenario will result in an impact given vulnerabilities, weaknesses, and predisposing conditions), (3) and the level of the impact [21].

[22] For additional information on cyber resiliency techniques and approaches, see SP 800-160v2r1, Appendix H [13].

2833 **Table 3. Effects of cyber resiliency techniques on adversarial threat events**

INTENDED EFFECT	IMPACT ON RISK	EXPECTED RESULTS
Redirect (includes deter, divert, and deceive): Direct threat events away from defender-chosen resources.	Reduce the likelihood of occurrence and (to a lesser extent) the likelihood of impact.	• The adversary's efforts cease. • The adversary actions are mistargeted or misinformed.
Deter Discourage the adversary from undertaking further activities by instilling fear (e.g., of attribution or retribution) or doubt that those activities would achieve their intended effects (e.g., that targets exist).	Reduce the likelihood of occurrence.	• The adversary ceases or suspends activities. **Example:** The defender uses disinformation to make it appear as though the organization is better able to detect attacks than it is and is willing to launch major counterstrikes. Therefore, the adversary chooses to not launch an attack due to fear of detection and reprisal.
Divert Direct the threat event toward defender-chosen resources.	Reduce the likelihood of occurrence.	• The adversary refocuses activities on defender-chosen resources. • The adversary directs activities toward targets beyond the defender's purview (e.g., other organizations). • The adversary does not affect resources that the defender has not selected to be targets. **Example:** The defender maintains an Internet-visible enclave with which untrusted external entities can interact and a private enclave accessible only via a VPN for trusted suppliers, partners, or customers (predefined segmentation). **Example:** The defender uses non-persistent information and obfuscation to hide critical resources combined with functional relocation of cyber resources and disinformation to lure the adversary toward a sandboxed enclave in which adversary actions cannot harm critical resources.
Deceive Lead the adversary to believe false information about defended systems, missions, organizations, or defender capabilities or TTPs.	Reduce the likelihood of occurrence and/or the likelihood of impact.	• The adversary's efforts are wasted as the assumptions on which the adversary bases their attacks are false. • The adversary takes actions based on false information, thus revealing that they have obtained that information. **Example:** The defender strategically places false information (disinformation) about the cybersecurity investments that it plans to make. As a result, the adversary's malware development is wasted by countering non-existent cybersecurity protections. **Example:** The defender uses selectively planted false information (disinformation) and honeynets (misdirection) to cause an adversary to focus its malware on virtual sandboxes while simultaneously employing obfuscation to hide the actual resources.
Preclude (includes expunge, preempt, and negate) Ensure that the threat event does not have an impact.	Reduce the likelihood of occurrence and/or the likelihood of impact.	• The adversary's efforts or resources cannot be applied or are wasted.

INTENDED EFFECT	IMPACT ON RISK	EXPECTED RESULTS
Expunge Remove resources that are known to be or are suspected of being unsafe, incorrect, or corrupted.	Reduce the likelihood of impact of subsequent events in the same threat scenario.	• A malfunctioning, misbehaving, or suspect resource is restored to normal operation. • The adversary loses a capability for some period as adversary-directed threat mechanisms (e.g., malicious code) are removed. • Adversary-controlled resources are so badly damaged that they cannot perform any function or be restored to a usable condition without being entirely rebuilt. **Example:** The defender uses virtualization to refresh critical software (non-persistent services) from a known good copy at random intervals (temporal unpredictability). As a result, malware that was implanted in the software is deleted.
Preempt Forestall or avoid conditions under which the threat event could occur or on which an attack is predicated.	Reduce the likelihood of occurrence.	• The adversary's resources cannot be applied, or the adversary cannot perform activities (e.g., because the resources that the adversary requires are destroyed or made inaccessible). **Example:** An unneeded network connection is disabled (non-persistent connectivity) so that an attack cannot be made via that interface. **Example:** A resource is repositioned (asset mobility) so it cannot be affected by a threat event in its new location.
Negate Create conditions under which the threat event cannot be expected to result in an impact.	Reduce the likelihood of impact.	• The adversary can launch an attack, but it will not even partially succeed. The adversary's efforts are wasted as the assumptions on which the adversary based its attack are no longer valid, and as a result, the intended effects cannot be achieved. **Example:** Subtle variations in critical software are implemented (synthetic diversity) with the result that the adversary's malware is no longer able to compromise the targeted software.
Impede (includes contain, degrade, delay, and exert) Make it more difficult for threat events to cause adverse impacts or consequences.	Reduce the likelihood and level of impact.	• Adversary activities are restricted in scope, fail to achieve full effect, do not take place in accordance with the adversary's timeline, or require greater resources than the adversary had planned.
Contain Restrict the effects of the threat event to a limited set of resources.	Reduce the level of impact.	• The adversary can affect fewer resources than planned. The value of the activity in achieving the adversary's goals is reduced. **Example:** The defender organization makes changes to a combination of internal firewalls and logically separated networks (dynamic segmentation) to isolate enclaves in response to the detection of malware with the result that the effects of the malware are limited to the initially infected enclaves.
Degrade Decrease the expected consequences of the threat event.	Reduce the likelihood of impact and/or the level of impact.	• Not all of the resources targeted by the adversary are affected, or the targeted resources are affected to a lesser degree than the adversary sought. **Example:** The defender uses multiple browsers and operating systems (architectural diversity) on end-user systems and some critical servers. The result is that malware targeted at specific software can only compromise a subset of the targeted systems, and a sufficient number continue to operate to complete the mission or business function.

INTENDED EFFECT	IMPACT ON RISK	EXPECTED RESULTS
Delay Increase the amount of time needed for the threat event to result in adverse impacts.	Reduce the likelihood of impact and/or the level of impact.	• The adversary achieves the intended effects but not within the intended period. **Example:** The protection measures (e.g., access controls, encryption) allocated to resources increase in number and strength based on resource criticality (calibrated defense-in-depth). The frequency of authentication challenges varies randomly (temporal unpredictability) and with increased frequency for more critical resources. The result is that it takes the attacker more time to successfully compromise the targeted resources.
Exert Increase the level of effort or resources needed for an adversary to achieve a given result.	Reduce the likelihood of impact.	• The adversary gives up planned or partially completed activities in response to finding that additional effort or resources are needed. • The adversary achieves the intended effects in their desired timeframe but only by applying more resources. Thus, the adversary's return on investment (ROI) is decreased. • The adversary reveals TTPs that they had planned to reserve for future use. **Example:** The defender enhances the defenses of moderate-criticality components with additional mitigations (calibrated defense-in-depth). To overcome these, the adversary must tailor and deploy TTPs that they were planning to reserve for use against higher value defender targets. **Example:** The defender adds a large amount of valid but useless information to a data store (obfuscation), requiring the adversary to exfiltrate and analyze more data before taking further actions.
Limit (includes shorten and reduce) Restrict the consequences of realized threat events by limiting the damage or effects they cause in terms of time, system resources, and/or mission or business impacts.	Reduce the level and likelihood of impact of subsequent events in the same threat scenario.	• The adversary's effectiveness is restricted.
Shorten Limit the duration of adverse consequences of a threat event.	Reduce the level of impact.	• The time period during which the adversary's activities affect defender resources is limited. **Example:** The defender employs a diverse set of suppliers (supply chain diversity) for time-critical components. As a result, when an adversary's attack on one supplier causes it to shut down, the defender can increase its use of the other suppliers, thus shortening the time when it is without the critical components.

INTENDED EFFECT	IMPACT ON RISK	EXPECTED RESULTS
Reduce Decrease the degree of damage from a threat event. The degree of damage can have two dimensions: breadth (i.e., number of affected resources) and depth (i.e., level of harm to a given resource).	Reduce the level of impact.	• The level of damage to mission or business operations due to adversary activities is reduced with partial restoration or the reconstitution of all affected resources. **Example:** Resources determined to be corrupted or suspect (integrity checks, behavior validation) are restored from older, uncorrupted resources (protected backup and restore) with reduced functionality. • The level of damage to mission or business operations due to adversary activities is reduced with the full restoration or reconstitution of some of the affected resources. **Example:** The organization removes one of three compromised resources and provides a new resource (replacement, specialization) for the same or equivalent mission or business functionality.
Expose (includes detect, scrutinize, and reveal) Reduce risk due to the ignorance of threat events and possible replicated or similar threat events in the same or similar environments.	Reduce the likelihood of impact.	• The adversary loses the advantage of stealth as defenders are better prepared by developing and sharing threat intelligence.
Detect Identify threat events or their effects by discovering or discerning the fact that an event is occurring, has occurred, or is about to occur based on indicators, warnings, and precursor activities.	Reduce the likelihood and level of impact, depending on responses.	• The adversary's activities become susceptible to defensive responses. **Example:** The defender continually moves its sensors (functional relocation of sensors), often at random times (temporal unpredictability), to common points of egress from the organization. They combine this with the use of beacon traps (tainting). The result is that the defender can quickly detect efforts by the adversary to exfiltrate sensitive information.
Scrutinize Analyze threat events and the artifacts associated with threat events—particularly with respect to patterns of exploiting vulnerabilities, predisposing conditions, and weaknesses—to inform more effective detection and risk response.	Reduce the likelihood of impact.	• The adversary loses the advantages of uncertainty, confusion, and doubt. • The defender understands the adversary better based on analysis of adversary activities, including the artifacts (e.g., malicious code) and effects associated with those activities and the correlation of activity-specific observations with other activities (as feasible), and can thus recognize adversary TTPs. **Example:** The defender deploys honeynets (misdirection), which invite attacks and allow the defender to apply their TTPs in a safe environment. The defender then analyzes (malware and forensic analysis) the malware captured in the honeynet to determine the nature of the attacker's TTPs, allowing it to develop appropriate defenses.

INTENDED EFFECT	IMPACT ON RISK	EXPECTED RESULTS
Reveal Increase the awareness of risk factors and the relative effectiveness of remediation approaches across the stakeholder community to support common, joint, or coordinated risk response.	Reduce the likelihood of impact, particularly in the future.	• The adversary loses the advantage of surprise and possible deniability. • The adversary's ability to compromise one organization's systems to attack another organization is impaired as awareness of adversary characteristics and behavior is increased across the stakeholder community (e.g., across all computer security incident response teams that support a given sector, that might be expected to be attacked by the same actor or actors). **Example:** The defender participates in threat information-sharing and uses dynamically updated threat intelligence data feeds (dynamic threat modeling) to inform actions (adaptive management).

2834

Appendix E. Organization-Defined Parameters

This appendix lists the organization-defined parameters (ODPs) that are included in the enhanced security requirements 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. Embedded ODPs are listed as a single entry in the table.

Table 4. Organization-defined parameters

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER
03.01.01E	[*Assignment: organization-defined privileged commands and/or other organization-defined actions*]
03.01.02E	[*Assignment: organization-defined restrictions*]
03.01.04E	[*Assignment: organization-defined account and/or account type*]
03.01.04E	[*Assignment: organization-defined number*]
03.01.08E	[*Assignment: organization-defined atypical usage*]
03.01.08E	[*Assignment: organization-defined personnel or roles*]
03.01.09E	[*Assignment: organization-defined attributes to assume access per*missions]
03.01.10E	[*Assignment: organization-defined security attributes*]
03.01.10E	[*Assignment: organization-defined information, source, and destination objects*]
03.01.10E	[*Assignment: organization-defined information flow control policies*]
03.02.01E	[*Assignment: organization-defined indicators of malicious code*]
03.02.01E	[*Assignment: organization-defined frequency*]
03.02.01E	[*Assignment: organization-defined events*]
03.02.03E	[*Assignment: organization-defined personnel*]
03.02.04E	[*Assignment: organization-defined personnel or roles*]
03.03.02E	[*Assignment: organization-defined real-time period*]
03.03.02E	[*Assignment: organization-defined personnel, roles, and/or locations*]
03.03.02E	[*Assignment: organization-defined audit logging failure events requiring real-time alerts*]
03.03.03E	[*Selection (one or more): movement; deletion*]
03.03.03E	[*Assignment: organization-defined audit information*]
03.03.04E	[*Selection (one or more): vulnerability scanning information; performance data; system monitoring information;* [*Assignment: organization-defined data/information collected from other sources*]]
03.04.02E	[*Assignment: organization-defined automated mechanisms*]
03.04.02E	[*Selection (one or more): disable network access by such components; isolate the components; notify* [*Assignment: organization-defined personnel or roles*]]
03.04.03E	[*Assignment: organization-defined automated mechanisms*]
03.04.04E	[*Assignment: organization-defined automated mechanisms*]
03.04.05E	[*Assignment: organization-defined system components and system-level information*]
03.04.06E	[*Assignment: organization-defined number*]
03.05.01E	[*Assignment: organization-defined devices and/or types of devices*]

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER
03.05.02E	[*Assignment: organization-defined password managers*]
03.05.03E	[*Assignment: organization-defined configuration management process*]
03.05.05E	[*Assignment: organization-defined time period*]
03.06.02E	[*Assignment: organization-defined time period*]
03.06.03E	[*Assignment: organization-defined environments or resources*]
03.06.04E	[*Assignment: organization-defined automated mechanisms*]
03.08.01E	[*Assignment: organization-defined system media containing CUI*]
03.08.02E	[*Assignment: organization-defined system backup information*]
03.09.03E	[*Assignment: organization-defined frequency*]
03.09.03E	[*Assignment: organization-defined frequency*]
03.10.01E	[*Assignment: organization-defined time period*]
03.10.01E	[*Assignment: organization-defined frequency*]
03.10.01E	[*Assignment: organization-defined personnel*]
03.10.03E	[*Assignment: organization-defined types of system components*]
03.11.02E	[*Assignment: organization-defined frequency*]
03.11.03E	[*Assignment: organization-defined systems or system components*]
03.11.03E	[*Assignment: organization-defined advanced automation and analytics capabilities*]
03.11.08E	[*Assignment: organization-defined means*]
03.11.09E	[*Assignment: organization-defined personnel or roles*]
03.11.09E	[*Assignment: organization-defined sources*]
03.11.10E	[*Assignment: organization-defined systems, system components, or system services*]
03.11.10E	[*Assignment: organization-defined decision points in the system development life cycle*]
03.11.11E	[*Assignment: organization-defined corrective actions*]
03.12.01E	[*Assignment: organization-defined frequency*]
03.12.01E	[*Assignment: organization-defined systems or system components*]
03.12.04E	[*Assignment: organization-defined system components or classes of components*]
03.12.04E	[*Assignment: organization-defined conditions*]
03.12.04E	[*Assignment: organization-defined frequency*]
03.13.01E	[*Assignment: organization-defined system components*]
03.13.02E	[*Assignment: organization-defined techniques*]
03.13.03E	[*Assignment: organization-defined concealment and misdirection techniques*]
03.13.04E	[*Assignment: organization-defined system components*]
03.13.05E	[*Assignment: organization-defined processing and/or storage*]
03.13.05E	[*Selection (one):* [*Assignment: organization-defined time frequency*]*; at random time intervals*]
03.13.06E	[*Assignment: organization-defined platform-independent applications*]
03.13.07E	[*Assignment: organization-defined frequency*]
03.13.09E	[*Assignment: organization-defined information security tools, mechanisms, and support components*]
03.13.11E	[*Assignment: organization-defined system components*]

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER
03.13.12E	[*Selection (one): Protect against; Limit*]
03.13.12E	[*Assignment: organization-defined types of denial-of-service events*]
03.13.12E	[*Assignment: organization-defined safeguards by type of denial-of-service event*]
03.13.13E	[*Selection (one): Physically; Logically*]
03.13.13E	[*Assignment: organization-defined connection ports or input/output devices*]
03.13.13E	[*Assignment: organization-defined systems or system components*]
03.13.14E	[*Assignment: organization-defined system, system component, or location*]
03.14.01E	[*Assignment: organization-defined software, firmware, and information*]
03.14.01E	[*Assignment: organization-defined actions*]
03.14.04E	[*Assignment: organization-defined trusted sources*]
03.14.05E	[*Selection (one): Refresh* [*Assignment: organization-defined information*] [*Assignment: organization-defined frequency*]*; Generate* [*Assignment: organization-defined information*] *on demand*]
03.14.08E	[*Assignment: organization-defined software, firmware, and information*]
03.14.08E	[*Selection (one or more): at startup; at* [*Assignment: organization-defined transitional states or security-relevant events*]*;* [*Assignment: organization-defined frequency*]]
03.14.10E	[*Assignment: organization-defined system components*]
03.14.10E	[*Assignment: organization-defined mechanisms*]
03.14.11E	[*Assignment: organization-defined security-relevant changes to the system*]
03.14.12E	[*Assignment: organization-defined information inputs to the system*]
03.14.13E	[*Assignment: organization-defined personnel or roles*]
03.14.14E	[*Assignment: organization-defined safeguards*]
03.14.15E	[*Assignment: organization-defined system components and services*]
03.14.15E	[*Selection (one or more): upon end of session of use; at* [*Assignment: organization-defined frequency*]]
03.14.16E	[*Assignment: organization-defined systems or system components*]
03.14.17E	[*Assignment: organization-defined personnel or roles*]
03.14.17E	[*Assignment: organization-defined compromise indicators*]
03.14.18E	[*Assignment: organization-defined personnel or roles*]
03.14.18E	[*Assignment: organization-defined activities that trigger alerts*]
03.15.01E	[*Assignment: organization-defined frequency*]
03.15.02E	[*Assignment: organization-defined security requirements*]
03.15.02E	[*Assignment: organization-defined architectural layers and locations*]
03.15.03E	[*Assignment: organization-defined safeguards*]
03.15.03E	[*Assignment: organization-defined locations and architectural layers*]
03.16.01E	[*Selection (one or more): design; modification; augmentation; reconfiguration*]
03.16.01E	[*Assignment: organization-defined systems or system components*]
03.17.01E	[*Selection (one or more): notification of supply chain compromises; results of assessments or audits; provision of* [*Assignment: organization-defined information*]]
03.17.02E	[*Selection (one or more): at random;* [*Assignment: organization-defined frequency*]*; upon* [*Assignment: organization-defined indications of need for inspection*]]

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER
03.17.02E	[*Assignment: organization-defined systems or system components*]
03.17.03E	[*Selection (one or more): source of counterfeit component;* [*Assignment: organization-defined external reporting organizations*]*;* [*Assignment: organization-defined personnel or roles*]]

Appendix F. Change Log

This publication incorporates the following changes from the original edition (February 2, 2021):

- Streamlined introductory information in Sec. 1 and Sec. 2 to improve clarity and understanding
- Increased the specificity of the enhanced security requirements to remove ambiguity, improve the effectiveness of implementation, and clarify the scope of assessments
- Grouped enhanced security requirements, where possible, to improve understanding and the efficiency of implementations and assessments
- Removed outdated and redundant enhanced security requirements
- Added new enhanced security requirements based on (1) the latest threat intelligence, (2) empirical data from cyber-attacks, and (3) the expansion of security objectives to include integrity and availability
- Added titles to the enhanced security requirements
- Restructured and streamlined the security requirement discussion sections
- Revised the enhanced security requirements for consistency with the security control language in SP 800-53
- Revised the structure of the References, Acronyms, and Glossary sections for greater clarity and ease of use
- Added Appendix C to summarize the enhanced security requirements
- Added Appendix E to list organization-defined parameters for the enhanced security requirements
- Removed an appendix with a mapping table for security controls and protection strategies and transferred that information to the individual security requirements in Sec. 3
- Implemented a one-time “revision number” change for consistency with SP 800-171r3

Table 5 shows the changes incorporated into this publication. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature. Any potential updates to this document that are not yet published in an errata update or a formal revision, including additional issues and potential corrections, will be posted as they are identified. See the publication details for this report. The current release of this publication does not include any errata updates.

Table 5. Change Log

PUBLICATION ID	DATE	TYPE OF EDIT	CHANGE	LOCATION