Enhanced Security Requirements for Protecting Controlled Unclassified Information

Initial Public Draft

Ron Ross

Victoria Pillitteri

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

Enhanced Security Requirements for Protecting Controlled Unclassified Information

Initial Public Draft

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

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~~ **January 17**, 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).

1   **Abstract**

2   The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and
3   organizations is of paramount importance to federal agencies and can directly impact the ability
4   of the Federal Government to successfully conduct its essential missions and functions. This
5   publication provides federal agencies with recommended security requirements for protecting
6   the confidentiality, integrity, and availability of CUI when it is resident in a nonfederal system
7   and organization and associated with a critical program or high value asset (HVA). The security
8   requirements apply to the components of nonfederal systems that process, store, or transmit
9   CUI or that provide protection for such components. The enhanced security requirements are
10   intended for use by federal agencies in contractual vehicles or other agreements established
11   between those agencies and nonfederal organizations.

12   **Keywords**

17   **Reports on Computer Systems Technology**

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

28 **Audience**

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

31 • System development life cycle responsibilities (e.g., program managers,
32 mission/business owners, information owners/stewards, system designers and
33 developers, system/security engineers, systems integrators)

34 • Acquisition or procurement responsibilities (e.g., contracting officers)

35 • System, security, or risk management and oversight responsibilities (e.g., authorizing
36 officials, chief information officers, chief information security officers, system owners,
37 information security managers)

38 • Security assessment and monitoring responsibilities (e.g., auditors, system evaluators,
39 assessors, independent verifiers/validators, analysts)

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

41 • *Federal perspective*: The entity establishing and conveying security assessment
42 requirements in contractual vehicles or other types of agreements

43 • *Nonfederal perspective*: The entity responding to and complying with the security
44 assessment requirements set forth in contracts or agreements

45   **Note to Reviewers**

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

54   • Streamlined introductory information in Sec. 1 and Sec. 2 to improve clarity and
55   understanding

56   • Increased specificity of the enhanced security requirements to remove ambiguity,
57   improve the effectiveness of implementation, and clarify the scope of assessments

58   • Grouped enhanced security requirements, where possible, to improve understanding
59   and the efficiency of implementations and assessments

60   • Removed outdated and redundant enhanced security requirements

61   • Added new enhanced security requirements based on (1) the latest threat intelligence,
62   (2) empirical data from cyber-attacks, and (3) the expansion of security objectives to
63   include integrity and availability

64   • Added new requirement families for consistency with SP 800-171r3, Revision 3: Planning
65   (PL), System and Services Acquisition (SA), and Supply Chain Risk Management (SR)

66   • Added titles to the enhanced security requirements

67   • Restructured and streamlined the security requirement discussion sections

68   • Revised the enhanced security requirements for consistency with the source security
69   control language in SP 800-53

70   • Revised the structure of the References, Acronyms, and Glossary sections for greater
71   clarity and ease of use

72   • Removed appendix with mapping table for security controls and protection strategies
73   and transferred information to the individual security requirements in Sec. 3

74   • Added new appendix that summarizes the enhanced security requirements

75   • Added new appendix that lists organization-defined parameters for the enhanced
76   security requirements

77   • Implemented a one-time "revision number" change for consistency with SP 800-171r3

78   **Call for Patent Claims**

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

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

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

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

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

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

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

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

104 Such statements should be addressed to: 800-171comments@list.nist.gov

105   **Table of Contents**

143   **List of Figures**

145   **Acknowledgments**

159   **1. Introduction**

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

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

181   In certain situations, CUI may be associated with a critical program[5] or a high value asset.[6]
182   These programs and assets are potential targets for the advanced persistent threat (APT). An
183   APT is an adversary or adversarial group that possesses the expertise and resources that allow it
184   to create opportunities to achieve its objectives by using multiple attack vectors, including
185   cyber, physical, and deception. APT objectives include establishing a foothold within the
186   infrastructure of targeted organizations exfiltrate information; undermine or impede critical
187   aspects of a mission, function, program, or organization; or position itself to carry out these
188   objectives in the future. The APT pursues its objectives repeatedly over an extended period,
189   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].

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

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

1.1. Purpose and Applicability

203   This publication provides federal agencies with a set of recommended enhanced security
204   requirements[8] for protecting the *confidentiality*, *integrity*, and *availability* of CUI when such
205   information is resident in nonfederal systems and organizations and where there are no specific
206   safeguarding requirements prescribed by the authorizing law, regulation, or government-wide
207   policy for the CUI category listed in the CUI registry [4].[9] The enhanced security requirements
208   address the protection of CUI by promoting penetration-resistant architecture, damage-limiting
209   operations, and cyber resiliency.[10] The requirements supplement the requirements in SP 800-
210   171 [12] and apply to components[11] of nonfederal systems that process, store, or transmit CUI
211   associated with a critical program or a high value asset or that provide protection for such
212   components. The requirements are intended for use by federal agencies in contractual vehicles
213   or other agreements that are established between those agencies and nonfederal
214   organizations.

215   Appropriately scoping security requirements is an important factor in determining protection-
216   related investment decisions and managing security risks for nonfederal organizations. If
217   nonfederal organizations designate specific system components to process, store, or transmit
218   CUI associated with a critical program or a high value asset, those organizations may limit the
219   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.

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

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

234 **1.2. Organization of This Publication**

235 The remainder of this publication is organized as follows:

236 • Section 2 describes the assumptions and methodology used to develop the enhanced
237   security requirements and the organization and structure of the requirements.

238 • Section 3 lists the enhanced security requirements for protecting the confidentiality,
239   integrity, and availability of CUI in nonfederal systems and organizations.

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

241 • References

242 • Appendix A: Acronyms

243 • Appendix B: Glossary

244 • Appendix C: Summary of Enhanced Security Requirements

245 • Appendix D: Adversary Effects

246 • Appendix E: Organization-Defined Parameters

247 • Appendix F: Change Log

248   **2. The Fundamentals**

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

252   **2.1. Enhanced Security Requirement Assumptions**

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

255   •   Federal information that is designated as CUI has the same value whether such
256   information resides in a federal or nonfederal system or organization.

257   •   Statutory and regulatory requirements for the protection of CUI are consistent in federal
258   and nonfederal systems and organizations.

259   •   Safeguards implemented to protect CUI are consistent in federal and nonfederal
260   systems and organizations.

261   •   The impact value for CUI is no less than *moderate*.[12]

262   •   The security requirements in SP 800-171 [12] have been satisfied to provide the
263   foundational level of protection for CUI.

264   •   Additional safeguards are necessary to protect CUI that is associated with critical
265   programs or high value assets.[13]

266   •   Nonfederal organizations can directly implement a variety of potential security solutions
267   or use external service providers to satisfy the security requirements.

268   **2.2. Enhanced Security Requirement Development Methodology**

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

271   •   *Penetration-resistant architecture:* An architecture that uses technology and procedures
272   to limit the opportunities for an adversary to compromise an organizational system and
273   to achieve a persistent presence in the system.

274   •   *Damage-limiting operations:* Procedural and operational measures that use system
275   capabilities to maximize the ability of an organization to detect successful system
276   compromises by an adversary and to limit the effects of such compromises (both
277   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.

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

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

290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
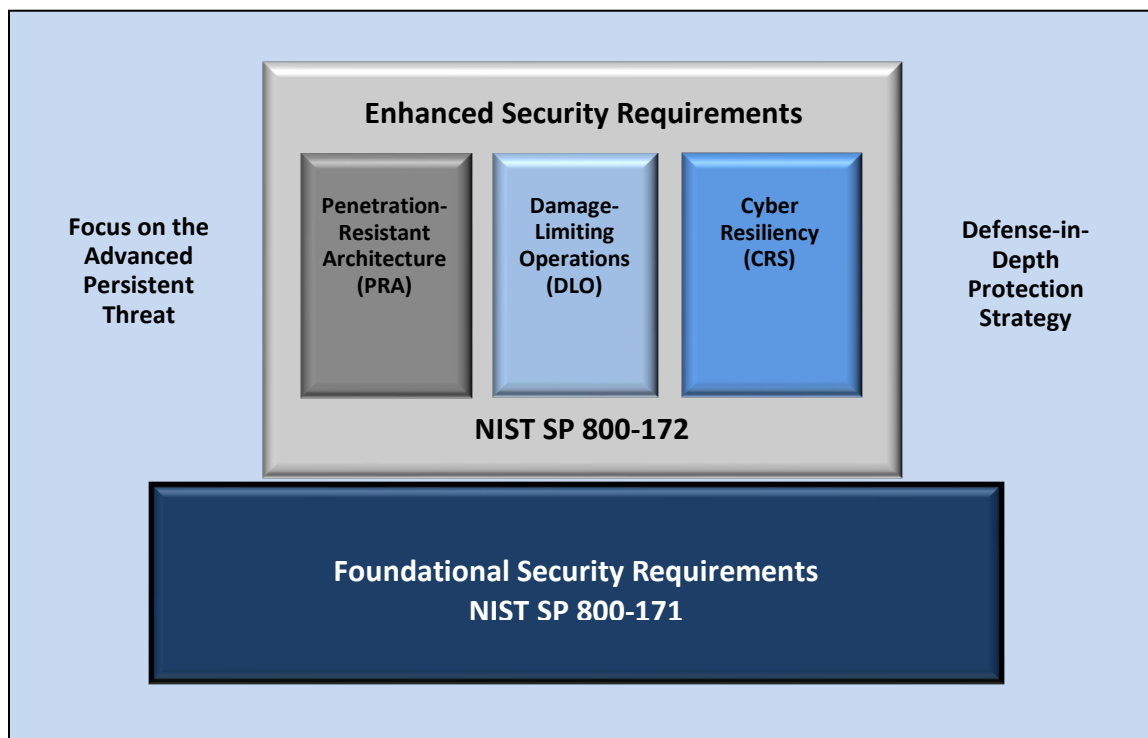
310   **Fig. 1. Multidimensional protection strategy**

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

315   •   Applying a threat-centric approach to security requirement specification

316   •   Employing system and security architectures that support logical and physical isolation
317   using system and network segmentation techniques, virtual machines, and containers

318   • Implementing dual authorization controls for critical or sensitive operations

319   • Limiting persistent storage to isolated enclaves or domains

320   • Implementing a comply-to-connect approach for systems and networks

321   • Extending configuration management requirements by establishing authoritative
322   sources for addressing changes to systems and system components

323   • Periodically refreshing or upgrading organizational systems and system components to a
324   known state or developing new systems or components

325   • Employing a security operations center with advanced analytics to support continuous
326   monitoring and the protection of systems

327   • Using deception to confuse and mislead adversaries regarding the information they use
328   for decision-making, the value and authenticity of the information they attempt to
329   exfiltrate, or the environment in which they are operating

330   Similar to the security requirements in SP 800-171 [12], the enhanced security requirements
331   are organized into 17 families, as illustrated in Table 1.

332   **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

333

334   Each family contains the security requirements related to the general security topic of the
335   family.[14] The structure of the security requirements is the same as the requirements in SP 800-
336   171 [12]. The enhanced security requirements are distinguished from the security requirements
337   in SP 800-171 by appending the letter "E" to the requirement numbers.

338   *Organization-defined parameters* (ODPs) are used in certain enhanced security requirements.
339   ODPs provide flexibility through the use of *assignment* and *selection* operations to allow federal
340   agencies and nonfederal organizations to specify values for the designated parameters in the
341   requirements.[15] Assignment and selection operations provide the capability to customize the
342   enhanced security requirements based on specific protection needs. The determination of ODP
343   values can be guided and informed by laws, Executive Orders, directives, regulations, policies,
344   standards, guidance, or mission and business needs. Once specified, the values for the ODPs
345   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.

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

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

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

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

367 **03.13.08E Decoys**

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

370 　　　　**DISCUSSION**

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

375 　　　　**PROTECTION STRATEGY**

376 　　　　DLO, CRS

377 　　　　**ADVERSARY EFFECTS**

378 　　　　Expose (Detect), Limit (Reduce)

379 　　　　**REFERENCES**

380 　　　　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.

381 **2.3. Enhanced Security Requirement Selection**

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

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

393 The security requirements for a nonfederal system processing, storing, or transmitting CUI that
394 is associated with a critical program or a high value asset are conveyed to the nonfederal
395 organization by the federal entity in a contract, grant, or other agreement. The implementation
396 guidance associated with the security requirements is beyond the scope of this publication.
397 Organizations have flexibility in the methods, techniques, technologies, and approaches used to
398 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.

399 **3. The Requirements**

400 This section describes enhanced security requirements that are designed to protect the
401 confidentiality, integrity, and availability of CUI in nonfederal systems and organizations. The
402 enhanced security requirements are not required for any particular category or article of CUI.
403 However, if a federal agency determines that CUI is associated with a critical program or a high
404 value asset, the CUI and the system that processes, stores, or transmits such information are
405 potential targets for the APT and, therefore, may require increased protection. Such protection
406 is expressed through the enhanced security requirements and is mandated by a federal agency
407 in a contract, grant, or other agreement. The enhanced security requirements are selected
408 either comprehensively or selectively in addition to the foundational requirements in SP 800-
409 171 [12].

410 Enhanced security requirements support one or more protection strategies with potential
411 effects on adversaries. The strategies and adversary effects are included in the supplementary
412 information for each enhanced security requirement to assist organizations in ascertaining
413 whether the requirement is appropriate. Ideally, the selected requirements should be balanced
414 across the three protection strategies. Selecting requirements that fall exclusively in one area
415 could result in an unbalanced response strategy for dealing with the APT. Similarly, with regard
416 to potential effects on adversaries, organizations should attempt to have as broad a set of
417 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.

418

---

419 **3.1. Access Control**

420 **03.01.01E Dual Authorization for Commands and Actions**

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

423   **DISCUSSION**

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

429 dual authorization duties to other individuals. Organizations also consider the risk
430 associated with implementing dual authorization when immediate responses are
431 necessary to ensure public and environmental safety. This requirement enhances SP
432 800-171 requirement 03.01.02.

433 **PROTECTION STRATEGY**

434 PRA

435 **ADVERSARY EFFECTS**

436 Preclude (Preempt), Impede (Exert)

437 **REFERENCES**

438 Source Control: AC-03(02)

439 **03.01.02E Non-Organizationally Owned Systems Restricted Use**

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

442 **DISCUSSION**

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

455 **PROTECTION STRATEGY**

456 PRA

457 **ADVERSARY EFFECTS**

458 Preclude (Preempt), Impede (Contain, Exert)

459 **REFERENCES**

460 Source Control: AC-20(03)

461   **03.01.03E Withdrawn**

462   Addressed by 03.01.09E, 03.01.10E, and 03.01.03.

463   **03.01.04E Concurrent Session Control**

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

466   **DISCUSSION**

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

474   **PROTECTION STRATEGY**

475   PRA

476   **ADVERSARY EFFECTS**

477   Preclude (Preempt), Impede (Contain, Exert)

478   **REFERENCES**

479   Source Control: AC-10

480   **03.01.05E Remote Access Monitoring and Control**

481   Implement automated mechanisms to monitor and control remote access methods.

482   **DISCUSSION**

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

488   **PROTECTION STRATEGY**

489   PRA, DLO

490   **ADVERSARY EFFECTS**

491   Preclude (Preempt), Impede (Exert)

492   **REFERENCES**

493   Source Control: AC-17(01)

494   **03.01.06E Protection of Remote Access Mechanism Information**

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

497   **DISCUSSION**

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

504   **PROTECTION STRATEGY**

505   PRA

506   **ADVERSARY EFFECTS**

507   Preclude (Preempt), Impede (Exert)

508   **REFERENCES**

509   Source Control: AC-17(06)

510   **03.01.07E Automated Actions for Account Management**

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

513   **DISCUSSION**

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

517   **PROTECTION STRATEGY**

518   PRA, DLO

519   **ADVERSARY EFFECTS**

520   Preclude (Preempt), Impede (Exert)

521   **REFERENCES**

522   Source Control: AC-02(04)

523   **03.01.08E Account Monitoring for Atypical Usage**

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

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

527   **DISCUSSION**

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

532   **PROTECTION STRATEGY**

533   DLO

534   **ADVERSARY EFFECTS**

535   Expose (Detect)

536   **REFERENCES**

537   Source Control: AC-02(12)

538   **03.01.09E Attribute-Based Access Control**

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

542   **DISCUSSION**

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

553   mandatory or discretionary form of access control. This requirement enhances SP
554   800-171 requirement 03.01.02.

555   **PROTECTION STRATEGY**

556   PRA

557   **ADVERSARY EFFECTS**

558   Preclude (Preempt), Impede (Exert)

559   **REFERENCES**

560   Source Control: AC-03(13)

561   **03.01.10E Object Security Attributes**

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

566   **DISCUSSION**

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

582   **PROTECTION STRATEGY**

583   PRA

584   **ADVERSARY EFFECTS**

585   Preclude (Preempt), Impede (Exert)

586	**REFERENCES**
587	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)

618 **03.02.02E Literacy and Awareness Training Practical Exercises**

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

620   **DISCUSSION**

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

628   **PROTECTION STRATEGY**

629   DLO

630   **ADVERSARY EFFECTS**

631   Preclude (Preempt), Expose (Detect)

632   **REFERENCES**

633   Source Control: AT-02(01)

634 **03.02.03E Literacy and Awareness Training Feedback**

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

637   **DISCUSSION**

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

643   **PROTECTION STRATEGY**

644   DLO

645   **ADVERSARY EFFECTS**

646   Preclude (Preempt), Expose (Detect)

647   **REFERENCES**

648   Source Control: AT-06

649 **03.02.04E Anti-Counterfeit Training**

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

652   **DISCUSSION**

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

655   **PROTECTION STRATEGY**

656   DLO

657   **ADVERSARY EFFECTS**

658   Preclude (Preempt), Expose (Detect)

659   **REFERENCES**

660   Source Control: SR-11(01)

661 **3.3. Audit and Accountability**

662 **03.03.01E Audit Record Storage in Separate Environment**

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

665   **DISCUSSION**

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

674   **PROTECTION STRATEGY**

675   DLO

676   **ADVERSARY EFFECTS**

677   Preclude (Preempt), Impede (Exert)

678   **REFERENCES**

679   Source Control: [AU-09(02)](#)

680   **03.03.02E   Real-Time Alerts for Audit Processing Failures**

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

685   **DISCUSSION**

686   Alerts provide organizations with urgent messages. Real-time alerts provide these
687   messages at information technology speed (i.e., the time from event detection to
688   alert occurs in seconds or less). This requirement enhances SP 800-171 requirement
689   03.03.04.

690   **PROTECTION STRATEGY**

691   DLO

692   **ADVERSARY EFFECTS**

693   Preclude (Preempt), Impede (Exert)

694   **REFERENCES**

695   Source Control: [AU-05(02)](#)

696   **03.03.03E   Dual Authorization for Audit Information and Actions**

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

699   **DISCUSSION**

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

709   **PROTECTION STRATEGY**

710   PRA

711   **ADVERSARY EFFECTS**

712   Preclude (Preempt), Impede (Exert)

713   **REFERENCES**

714   Source Control: AU-09(05)

715   **03.03.04E Integrated Analysis of Audit Records**

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

721   **DISCUSSION**

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

737   **PROTECTION STRATEGY**

738   DLO

739   **ADVERSARY EFFECTS**

740   Preclude (Preempt), Expose (Detect)

741   **REFERENCES**

742   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)

773   **03.04.03E Automation Support for System Component Inventory**

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

777   **DISCUSSION**

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

793   **PROTECTION STRATEGY**

794   PRA, DLO

795   **ADVERSARY EFFECTS**

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

797   **REFERENCES**

798   Source Control: CM-08(02)

799   **03.04.04E Automation Support for Baseline Configuration**

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

803   **DISCUSSION**

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

808　applications, the types of software installed, and current patch levels. Automation
809　support for accuracy and currency can be satisfied by the implementation of
810　03.04.03E for organizations that combine system component inventory and baseline
811　configuration activities. This requirement enhances SP 800-171 requirement
812　03.04.01.

813　**PROTECTION STRATEGY**

814　PRA, DLO

815　**ADVERSARY EFFECTS**

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

817　**REFERENCES**

818　Source Control: CM-02(02)

819　**03.04.05E　Dual Authorization for System Changes**

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

822　**DISCUSSION**

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

834　**PROTECTION STRATEGY**

835　PRA

836　**ADVERSARY EFFECTS**

837　Preclude (Preempt), Impede (Exert)

838　**REFERENCES**

839　Source Control: CM-5(04)

840 **03.04.06E Retention of Previous Configurations**

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

843   **DISCUSSION**

844   Retaining previous versions of baseline configurations to support rollback includes
845   hardware, software, and firmware configuration files, configuration records, and
846   associated documentation. This requirement enhances SP 800-171 requirement
847   03.04.01.

848   **PROTECTION STRATEGY**

849   PRA, CRS

850   **ADVERSARY EFFECTS**

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

852   **REFERENCES**

853   Source Control: [CM-02(03)](CM-02(03))

854 **03.04.07E Testing, Validation, and Documentation of Changes**

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

857   **DISCUSSION**

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

869   **PROTECTION STRATEGY**

870   PRA

871   **ADVERSARY EFFECTS**

872   Preclude (Preempt), Impede (Exert)

873   **REFERENCES**

874   Source Control: CM-03(02)

875   **3.5. Identification and Authentication**

876   **03.05.01E Cryptographic Bidirectional Authentication**

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

880   **DISCUSSION**

881   Bidirectional authentication provides stronger protection to validate the identity of
882   other devices for connections that are of greater risk. The requirement applies to
883   client-server authentication, server-server authentication, and device authentication
884   (including mobile devices). The cryptographic key for authentication transactions is
885   stored in secure storage that is available to the authenticator application (e.g.,
886   keychain storage, Trusted Platform Module (TPM), Trusted Execution Environment
887   (TEE), or secure element). This requirement enhances SP 800-171 requirement
888   03.05.02.

889   **PROTECTION STRATEGY**

890   PRA

891   **ADVERSARY EFFECTS**

892   Preclude (Preempt, Negate), Expose (Detect)

893   **REFERENCES**

894   Source Controls: IA-03(01)

895   **03.05.02E Password Managers**

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

898   **DISCUSSION**

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

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

907   **PROTECTION STRATEGY**

908   PRA

909   **ADVERSARY EFFECTS**

910   Preclude (Preempt), Impede (Delay, Exert)

911   **REFERENCES**

912   Source Control: IA-05(18)

913   **03.05.03E Device Attestation**

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

916   **DISCUSSION**

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

927   **PROTECTION STRATEGY**

928   PRA

929   **ADVERSARY EFFECTS**

930   Preclude (Preempt), Impede (Exert)

931   **REFERENCES**

932   Source Control: IA-03(04)

933   **03.05.04E Embedded Unencrypted Static Authenticators**

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

936   **DISCUSSION**

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

942   **PROTECTION STRATEGY**

943   PRA

944   **ADVERSARY EFFECTS**

945   Preclude (Preempt), Impede (Exert)

946   **REFERENCES**

947   Source Control: IA-05(07)

948   **03.05.05E Expiration of Cached Authenticators**

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

951   **DISCUSSION**

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

956   **PROTECTION STRATEGY**

957   PRA

958   **ADVERSARY EFFECTS**

959   Preclude (Preempt), Impede (Exert)

960   **REFERENCES**

961   Source Control: IA-05(13)

962   **03.05.06E Identity Proofing**

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

966   b.   Resolve user identities to a unique individual.

967   c.   Collect, validate, and verify identity evidence.

968   **DISCUSSION**

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

974   **PROTECTION STRATEGY**

975   PRA

976   **ADVERSARY EFFECTS**

977   Preclude (Preempt), Impede (Exert)

978   **REFERENCES**

979   Source Control: IA-12

980   **3.6. Incident Response**

981   **03.06.01E Security Operations Center**

982   Establish and maintain a security operations center.

983   **DISCUSSION**

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

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

1000   **PROTECTION STRATEGY**

1001   DLO

1002   **ADVERSARY EFFECTS**

1003   Limit (Shorten, Reduce); Expose (Detect)

1004   **REFERENCES**

1005   Source Control: IR-4(14)

1006   **03.06.02E Integrated Incident Response Team**

1007   Establish and maintain an integrated incident response team that can be deployed
1008   to any location identified by the organization in [*Assignment: organization-defined*
1009   *time period*].

1010   **DISCUSSION**

1011   An integrated incident response team is a group of individuals who assess,
1012   document, and respond to incidents so that organizational systems and networks
1013   can recover quickly and implement the necessary controls to avoid future incidents.
1014   Incident response team personnel include forensic and malicious code analysts,
1015   systems security engineers, tool developers, and real-time operations personnel.
1016   The incident handling capability includes performing rapid forensic preservation of
1017   evidence and analysis of and response to intrusions.

1018   An integrated incident response team facilitates information sharing and allows
1019   organizational personnel (e.g., developers, implementers, and operators) to leverage
1020   team knowledge of the threat and implement defensive measures that enable
1021   organizations to deter intrusions more effectively. Moreover, integrated teams
1022   promote the rapid detection of intrusions, the development of appropriate
1023   mitigations, and the deployment of effective defensive measures. Integrated
1024   incident response teams are better able to identify adversary tactics, techniques,
1025   and procedures (TTP) that are linked to the operations tempo or specific mission and
1026   business functions and to define responsive actions in a way that does not disrupt
1027   those mission and business functions. Incident response teams can be distributed
1028   within organizations to make the capability resilient. For some organizations, the
1029   incident response team can be a cross-organizational entity. This requirement
1030   enhances SP 800-171 requirement 03.06.01.

1031   **PROTECTION STRATEGY**

1032   DLO

1033   **ADVERSARY EFFECTS**

1034   Preclude (Expunge), Impede (Contain, Exert), Limit (Shorten, Reduce), Expose
1035   (Scrutinize)

1036   **REFERENCES**

1037   Source Control: IR-4(11)

1038 **03.06.03E** **Behavior Analysis**

1039   Analyze anomalous or suspected adversarial behavior in or related to [*Assignment:*
1040   *organization-defined environments or resources*].

1041   **DISCUSSION**

1042   If the organization maintains a deception environment, an analysis of behaviors in
1043   that environment, including resources targeted by the adversary and the timing of
1044   the incident or event, can provide significant insights into adversarial TTPs. External
1045   to a deception environment, the analysis of anomalous adversarial behavior (e.g.,
1046   changes in system performance or usage patterns) or suspected behavior (e.g.,
1047   changes in searches for the location of specific resources) can give the organization
1048   such insight. This requirement enhances SP 800-171 requirement 03.06.01.

1049   **PROTECTION STRATEGY**

1050   DLO

1051   **ADVERSARY EFFECTS**

1052   Expose (Detect, Reveal)

1053   **REFERENCES**

1054   Source Control: IR-04(13)

1055 **03.06.04E** **Automation Support for Incident Reporting**

1056   Track incidents, and collect and analyze incident information using [*Assignment:*
1057   *organization-defined automated mechanisms*].

1058   **DISCUSSION**

1059   Automated mechanisms for tracking incidents and collecting and analyzing incident
1060   information include Computer Incident Response Centers or other electronic

1061   databases of incidents and network monitoring devices. This requirement enhances
1062   SP 800-171 requirement 03.06.02.

1063   **PROTECTION STRATEGY**

1064   PRA, DLO

1065   **ADVERSARY EFFECTS**

1066   Expose (Detect, Reveal)

1067   **REFERENCES**

1068   Source Control: IR-05(01)

1069   **3.7. Maintenance**

1070   **03.07.01E Maintenance Tool Software Updates and Patches**

1071   Inspect maintenance tools to ensure the latest software updates and patches are
1072   installed.

1073   **DISCUSSION**

1074   Maintenance tools using outdated and/or unpatched software can provide a threat
1075   vector for adversaries and result in a significant vulnerability for organizations. This
1076   requirement enhances SP 800-171 requirement 03.07.04.

1077   **PROTECTION STRATEGY**

1078   PRA

1079   **ADVERSARY EFFECTS**

1080   Preclude (Preempt)

1081   **REFERENCES**

1082   Source Control: MA-03(06)

1083   **3.8. Media Protection**

1084   **03.08.01E Dual Authorization for Media Sanitization**

1085   Enforce dual authorization for the sanitization of [*Assignment: organization-defined*
1086   *system media containing CUI*].

1087 **DISCUSSION**

1088 Dual authorization is also known as two-person control. Dual authorization reduces
1089 risk related to insider threats, including adversaries who have obtained credentials.
1090 Organizations employ dual authorization to help ensure that the sanitization of
1091 system media cannot occur unless two technically qualified individuals conduct the
1092 designated task. Individuals who sanitize system media possess sufficient skills and
1093 expertise to determine whether the proposed sanitization reflects applicable federal
1094 and organizational standards, policies, and procedures. Dual authorization also helps
1095 to ensure that sanitization occurs as intended to protect against errors and false
1096 claims of having performed the sanitization actions. To reduce the risk of collusion,
1097 organizations consider rotating dual authorization duties to other individuals.
1098 Organizations consider the risks associated with implementing dual authorization
1099 when immediate responses are necessary to help ensure public and environmental
1100 safety. This requirement enhances SP 800-171 requirement 03.08.03.

1101 **PROTECTION STRATEGY**

1102 PRA

1103 **ADVERSARY EFFECTS**

1104 Preclude (Preempt), Impede (Exert)

1105 **REFERENCES**

1106 Source Control: MP-06(07)

1107 **03.08.02E Dual Authorization for System Backup Deletion and Destruction**

1108 Enforce dual authorization for the deletion or destruction of [*Assignment:*
1109 *organization-defined system backup information*].

1110 **DISCUSSION**

1111 Dual authorization is also known as two-person control. Dual authorization reduces
1112 risk related to insider threats, including adversaries who have obtained credentials.
1113 Dual authorization ensures that the deletion or destruction of backup information
1114 cannot occur unless two qualified individuals carry out the task. Individuals who
1115 delete or destroy backup information possess the knowledge, skills, or expertise to
1116 determine whether the proposed deletion or destruction of such information
1117 reflects organizational policies and procedures. To reduce the risk of collusion,
1118 organizations consider rotating dual authorization duties to other individuals.
1119 Organizations also consider the risk associated with implementing dual authorization
1120 when immediate responses are necessary to ensure public and environmental
1121 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.

1150   **03.09.02E Withdrawn**

1151   Addressed by [03.01.01](#) and [03.09.01](#).

1152   **03.09.03E Access Agreements**

1153   a. Develop and document access agreements for systems processing, storing, or
1154   transmitting CUI.

1155   b. Review and update the access agreements [*Assignment: organization-defined*
1156   *frequency*].

1157   c. Verify that individuals requiring access to CUI and systems processing, storing, or
1158   transmitting CUI:

1159   1. Sign appropriate access agreements prior to being granted access; and

1160   2. Re-sign access agreements to maintain access to systems when access
1161   agreements have been updated or [*Assignment: organization-defined*
1162   *frequency*].

1163   **DISCUSSION**

1164   Access agreements include nondisclosure agreements, acceptable use agreements,
1165   rules of behavior, and conflict-of-interest agreements. Signed access agreements
1166   include an acknowledgement that individuals have read, understand, and agree to
1167   abide by the constraints associated with systems processing, storing, or transmitting
1168   CUI to which they have authorized access.

1169   **PROTECTION STRATEGY**

1170   PRA

1171   **ADVERSARY EFFECTS**

1172   Preclude (Preempt)

1173   **REFERENCES**

1174   Source Control: [PS-06](#)

1175   **03.09.04E Citizenship Requirements**

1176   Verify that individuals accessing a system processing, storing, or transmitting CUI are
1177   U.S. citizens.

1178   **DISCUSSION**

1179   Organizations may determine that individuals who need access to CUI associated
1180   with a high value asset or critical program require U.S. citizenship status. This
1181   requirement enhances SP 800-171 requirement 03.09.01.

1182   **PROTECTION STRATEGY**

1183   PRA

1184   **ADVERSARY EFFECTS**

1185   Preclude (Preempt)

1186   **REFERENCES**

1187   Source Control: PS-03(04)

1188   **3.10. Physical Protection**

1189   **03.10.01E   Visitor Access Records**

1190   a.   Maintain visitor access records to the facility where the system resides
1191   for [*Assignment: organization-defined time period*].

1192   b.   Review visitor access records [*Assignment: organization-defined frequency*].

1193   c.   Report anomalies in visitor access records to [*Assignment: organization-defined*
1194   *personnel*].

1195   **DISCUSSION**

1196   Visitor access records include the names and organizations of individuals visiting,
1197   visitor signatures, forms of identification, dates of access, entry and departure times,
1198   purpose of visits, and the names and organizations of individuals visited. Access
1199   record reviews determine whether access authorizations are current and still
1200   required to support organizational mission and business functions. Access records
1201   are not required for publicly accessible areas.

1202   **PROTECTION STRATEGY**

1203   PRA

1204   **ADVERSARY EFFECTS**

1205   Preclude (Preempt)

1206   **REFERENCES**

1207   Source Control: PE-08

1208 **03.10.02E Intrusion Alarms and Surveillance Equipment**

1209 Monitor physical access to the facility where the system resides using physical
1210 intrusion alarms and surveillance equipment.

1211 **DISCUSSION**

1212 Physical intrusion alarms can be used to alert security personnel when unauthorized
1213 access to the facility is attempted. Alarm systems work in conjunction with physical
1214 barriers, physical access control systems, and facility security guards by triggering a
1215 response when these other forms of security have been compromised or breached.
1216 Physical intrusion alarms can include different types of sensor devices, including
1217 motion sensors, contact sensors, and broken glass sensors. Surveillance equipment
1218 includes video cameras installed at strategic locations throughout the facility. This
1219 requirement enhances SP 800-171 requirement 03.10.02.

1220 **PROTECTION STRATEGY**

1221 DLO

1222 **ADVERSARY EFFECTS**

1223 Expose (Detect, Reveal)

1224 **REFERENCES**

1225 Source Control: PE-06(01)

1226 **03.10.03E Delivery and Removal of System Components**

1227 a. Authorize and control [*Assignment: organization-defined types of system
1228 components*] entering and exiting the facility.

1229 b. Maintain records of the system components.

1230 **DISCUSSION**

1231 Enforcing authorizations for the entry and exit of system components may require
1232 restricting access to delivery areas and isolating the areas from the system and
1233 media libraries.

1234 **PROTECTION STRATEGY**

1235 PRA

1236 **ADVERSARY EFFECTS**

1237 Preclude (Preempt)

1238   **REFERENCES**

1239   Source Control: [PE-16]

1240   **3.11. Risk Assessment**

1241   **03.11.01E Threat Awareness Program**

1242   Implement a threat awareness program that includes a cross-organization
1243   information-sharing capability for threat intelligence.

1244   **DISCUSSION**

1245   Because of the constantly changing and increasing sophistication of adversaries,
1246   especially the advanced persistent threat (APT), it may be likely that adversaries can
1247   successfully breach or compromise organizational systems. One of the techniques
1248   that organizations can use to address this concern is to share threat information,
1249   including threat events (i.e., tactics, techniques, and procedures) that organizations
1250   have experienced, mitigations that organizations have found to be effective against
1251   certain types of threats, and threat intelligence (i.e., indications and warnings about
1252   threats). Threat information sharing may be bilateral or multilateral. Bilateral threat
1253   sharing can include government-to-commercial and government-to-government
1254   cooperatives. Multilateral threat sharing can include organizations taking part in
1255   threat-sharing consortia. Threat information may require special agreements and
1256   protection, or it may be freely shared.

1257   To maximize the effectiveness of monitoring and sharing threat intelligence
1258   information, it is important to know what threat observables and indicators the
1259   sensors need to be searching for. By using well-established frameworks, services,
1260   and automated tools, organizations improve their ability to rapidly share and feed
1261   the relevant threat detection signatures into monitoring tools.

1262   **PROTECTION STRATEGY**

1263   DLO

1264   **ADVERSARY EFFECTS**

1265   Preclude (Negate), Impede (Exert), Expose (Detect)

1266   **REFERENCES**

1267   Source Controls: [PM-16]

1268   **03.11.02E Threat Hunting**

1269   a. Establish and maintain a cyber threat hunting capability to:

1270   1. Search for indicators of compromise in organizational systems and

1271   2. Detect, track, and disrupt threats that evade existing controls.

1272   b. Implement the threat hunting capability [*Assignment: organization-defined
1273   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

1305   machine learning. Examples include automated workflow operations; automated
1306   threat discovery and response, including broad-based collection, context-based
1307   analysis, and adaptive response capabilities; and machine-assisted decision tools.
1308   However, sophisticated adversaries may be able to extract information related to
1309   analytic parameters and retrain the machine learning to classify malicious activity as
1310   benign. Accordingly, machine learning is augmented by human monitoring to ensure
1311   that sophisticated adversaries are not able to conceal their activities. This
1312   requirement enhances SP 800-171 requirement 03.11.01.

1313   **PROTECTION STRATEGY**

1314   DLO

1315   **ADVERSARY EFFECTS**

1316   Preclude (Expunge), Limit (Shorten, Reduce), Expose (Detect, Scrutinize)

1317   **REFERENCES**

1318   Source Control: RA-03(04)

1319   **03.11.04E Withdrawn**

1320   Addressed by 03.15.01E, 03.15.02.

1321   **03.11.05E Withdrawn**

1322   Addressed by 03.11.01E, 03.11.01, and 03.12.01.

1323   **03.11.06E Withdrawn**

1324   Addressed by 03.12.03E, 03.17.03E, 03.11.01, and 03.11.04.

1325   **03.11.07E Withdrawn**

1326   Addressed by 03.17.01.

1327   **03.11.08E Dynamic Threat Awareness**

1328   Determine the current cyber threat environment on an ongoing basis using
1329   [*Assignment: organization-defined means*].

1330   **DISCUSSION**

1331   The threat awareness information that is gathered feeds into the organization's
1332   security operations to ensure that procedures are updated in response to the
1333   changing threat environment. For example, at higher threat levels, organizations

1334   may change the privilege or authentication thresholds required to perform certain
1335   operations. This requirement enhances SP 800-171 requirement 03.11.01.

1336   **PROTECTION STRATEGY**

1337   DLO

1338   **ADVERSARY EFFECTS**

1339   Expose (Detect, Reveal)

1340   **REFERENCES**

1341   Source Control: RA-03(03)

1342   **03.11.09E Indicators of Compromise**

1343   Discover, collect, and distribute to [*Assignment: organization-defined personnel or
1344   roles*], indicators of compromise provided by [*Assignment: organization-defined
1345   sources*].

1346   **DISCUSSION**

1347   Indicators of compromise (IOCs) are forensic artifacts from intrusions that are
1348   identified on organizational systems at the host or network level. IOCs provide
1349   valuable information on systems that have been compromised. IOCs can include the
1350   creation of registry key values. IOCs for network traffic include universal resource
1351   locator (URL) or protocol elements that indicate malicious code command and
1352   control servers. The rapid distribution and adoption of IOCs can improve information
1353   security by reducing the time that systems and organizations are vulnerable to the
1354   same exploit or attack. Threat indicators, signatures, TTPs, and other IOCs may be
1355   available via government and non-government cooperatives, including the Forum of
1356   Incident Response and Security Teams (FIRST), the Computer Emergency Response
1357   Team (CERT) Coordination Center (CERTCC), the United States Computer Emergency
1358   Readiness Team, and the Defense Industrial Base (DIB) Cybersecurity Information
1359   Sharing Program. This requirement enhances SP 800-171 requirement 03.14.06. It is
1360   also related to 03.11.02.

1361   **PROTECTION STRATEGY**

1362   DLO

1363   **ADVERSARY EFFECTS**

1364   Expose (Detect, Reveal)

1365   **REFERENCES**

1366   Source Control: SI-04(24)

1367   **03.11.10E Criticality Analysis**

1368   Identify critical system components and functions by performing a criticality analysis
1369   for [*Assignment: organization-defined systems, system components, or system*
1370   *services*] at [*Assignment: organization-defined decision points in the system*
1371   *development life cycle*].

1372   **DISCUSSION**

1373   Not all system components, functions, or services necessarily require significant
1374   protection. For example, criticality analysis is a key tenet of risk management and
1375   informs the prioritization of protection activities. The identification of critical system
1376   components and functions considers applicable laws, Executive Orders, regulations,
1377   directives, policies, standards, system functionality requirements, as well as system
1378   and system component interfaces and dependencies. Organizations conduct a
1379   functional decomposition of a system to identify mission-critical functions and
1380   system components. The functional decomposition includes the identification of
1381   organizational missions supported by the system, decomposition into the specific
1382   functions to perform those missions, and traceability to the hardware, software, and
1383   firmware components that implement those functions, including when the functions
1384   are shared by many components within and external to the system.

1385   The operational environment of a system or a system component may impact the
1386   criticality, including the connections to and dependencies on cyber-physical systems,
1387   devices, system-of-systems, and outsourced IT services. System components that
1388   allow unmediated access to critical system components or functions are considered
1389   critical due to the inherent vulnerabilities that such components create. Function
1390   and component criticality are assessed in terms of the impact of a function or
1391   component failure on the organizational missions that are supported by the system
1392   that contains the functions and components.

1393   Criticality analysis is performed when an architecture or design is being developed,
1394   modified, or upgraded. If such analysis is performed early and throughout the
1395   system development life cycle, organizations may be able to modify the system
1396   design to reduce the critical nature of these functions and components, such as by
1397   adding redundancy or alternate paths into the system design. Criticality analysis can
1398   also influence the protection measures required by development contractors. In
1399   addition to criticality analysis for systems, system components, and system services,
1400   criticality analysis of information is an important consideration.

1401   **PROTECTION STRATEGY**

1402   PRA

1403   **ADVERSARY EFFECTS**

1404   Preclude (Preempt)

1405   **REFERENCES**

1406   Source Control: RA-09

1407   **03.11.11E Discoverable Information**

1408   Determine information about the system that is discoverable and take [*Assignment:*
1409   *organization-defined corrective actions*].

1410   **DISCUSSION**

1411   Discoverable information includes information that adversaries could obtain without
1412   compromising or breaching the system, such as by collecting information that the
1413   system is exposing or by conducting extensive web searches. Corrective actions
1414   include notifying organizational personnel, removing designated information, or
1415   changing the system to make the designated information less relevant or attractive
1416   to adversaries. This requirement excludes intentionally discoverable information
1417   that may be part of a decoy capability (e.g., honeypots, honeynets, or deception
1418   nets) implemented by the organization. This requirement enhances SP 800-171
1419   requirement 03.11.02.

1420   **PROTECTION STRATEGY**

1421   DLO

1422   **ADVERSARY EFFECTS**

1423   Expose (Reveal)

1424   **REFERENCES**

1425   Source Control: RA-05(04)

1426   **03.11.12E Automated Means for Sharing Threat Intelligence**

1427   Implement automated mechanisms to maximize the effectiveness of sharing threat
1428   intelligence information.

1429   **DISCUSSION**

1430   To maximize the effectiveness of monitoring and sharing threat intelligence
1431   information, it is important to know what threat observables and indicators the
1432   sensors need to be searching for. By using well-established frameworks, services,
1433   and automated tools, organizations improve their ability to rapidly share and feed
1434   the relevant threat detection signatures into monitoring tools.

1435   **PROTECTION STRATEGY**

1436   DLO

1437   **ADVERSARY EFFECTS**

1438   Preclude (Negate), Impede (Exert), Expose (Detect)

1439   **REFERENCES**

1440   Source Controls: PM-16(01)

1441   **3.12. Security Assessment and Monitoring**

1442   **03.12.01E Penetration Testing**

1443   Conduct penetration testing [*Assignment: organization-defined frequency*] on
1444   [*Assignment: organization-defined systems or system components*].

1445   **DISCUSSION**

1446   Penetration testing is a specialized type of assessment conducted on systems or
1447   individual system components to identify vulnerabilities that could be exploited by
1448   adversaries. Penetration testing goes beyond automated vulnerability scanning. It is
1449   conducted by penetration testing agents and teams with particular skills and
1450   experience that include technical expertise in network, operating system, and
1451   application-level security. Penetration testing can be used to validate vulnerabilities
1452   or determine a system's penetration resistance to adversaries within specified
1453   constraints, such as time, resources, and skills. Organizations may also supplement
1454   penetration testing with red team exercises. Red teams attempt to duplicate the
1455   actions of adversaries in carrying out attacks against organizations and provide an in-
1456   depth analysis of security-related weaknesses or deficiencies.

1457   Organizations can use the results of vulnerability analyses to support penetration
1458   testing activities. Penetration testing can be conducted internally or externally on
1459   the hardware, software, or firmware components of a system and can exercise both
1460   physical and technical controls. A standard method for penetration testing includes
1461   pretest analysis based on full knowledge of the system, pretest identification of
1462   potential vulnerabilities based on the pretest analysis, and testing designed to
1463   determine the exploitability of vulnerabilities. All parties agree to the specified rules
1464   of engagement before the commencement of penetration testing. Organizations
1465   correlate the rules of engagement for penetration tests and red teaming exercises (if
1466   used) with the tools, techniques, and procedures that they anticipate adversaries
1467   may employ. The penetration testing or red team exercises may be organization-
1468   based or external to the organization. In either case, it is important that the team
1469   possesses the necessary skills and resources to do the job and is objective in its
1470   assessment.

1471   **PROTECTION STRATEGY**

1472   PRA, DLO

1473   **ADVERSARY EFFECTS**

1474   Preclude (Preempt), Impede (Exert), Expose (Detect)

1475   **REFERENCES**

1476   Source Control: CA-08

1477   **03.12.02E Independent Assessors**

1478   Use independent assessors or assessment teams to conduct security requirement
1479   assessments.

1480   **DISCUSSION**

1481   Independent assessors or assessment teams are individuals or groups who conduct
1482   impartial assessments of systems. Impartiality means that assessors are free from
1483   any perceived or actual conflicts of interest regarding the development, operation,
1484   sustainment, or management of the systems under assessment or the determination
1485   of security requirement effectiveness. To achieve impartiality, assessors do not
1486   create a mutual or conflicting interest with the organizations where the assessments
1487   are being conducted, assess their own work, act as management or employees of
1488   the organizations they are serving, or place themselves in positions of advocacy for
1489   the organizations acquiring their services.

1490   Independent assessments can be obtained from elements within organizations or be
1491   contracted to entities outside of organizations. Organizational officials determine
1492   the required level of independence based on the risk to organizational operations,
1493   organizational assets, or individuals. Organizational officials also determine whether
1494   the level of assessor independence provides sufficient assurance such that the
1495   assessment results are sound and can be used to make effective risk-based
1496   decisions. Independence determination includes whether contracted assessment
1497   services have sufficient independence, such as when system owners are not directly
1498   involved in the contracting processes or cannot influence the impartiality of the
1499   assessors conducting the assessments. During the system design and development
1500   phase, having independent assessors is analogous to having independent subject-
1501   matter experts involved in design reviews.

1502   When the structures of the organizations require that assessments be conducted by
1503   individuals that are in the developmental, operational, or management chain of the
1504   system owners, independence in assessment processes can be achieved by ensuring
1505   that assessment results are carefully reviewed and analyzed by independent teams

1506   of experts to validate the completeness, accuracy, integrity, and reliability of the
1507   results. This requirement enhances SP 800-171 requirement 03.12.01.

1508   **PROTECTION STRATEGY**

1509   PRA

1510   **ADVERSARY EFFECTS**

1511   Preclude (Preempt)

1512   **REFERENCES**

1513   Source Control: CA-02(01)

1514   **03.12.03E Risk Monitoring**

1515   Ensure risk monitoring is an integral part of the continuous monitoring strategy that
1516   includes effectiveness monitoring, compliance monitoring, change monitoring.

1517   **DISCUSSION**

1518   Risk monitoring is guided and informed by the established organizational risk
1519   tolerance. Effectiveness monitoring determines the ongoing effectiveness of the
1520   implemented risk response measures. Compliance monitoring verifies that required
1521   risk response measures are implemented. It also verifies that security requirements
1522   are satisfied. Change monitoring identifies changes to organizational systems and
1523   environments of operation that may affect security risk. This requirement enhances
1524   SP 800-171 requirement 03.12.03.

1525   **PROTECTION STRATEGY**

1526   PRA, DLO

1527   **ADVERSARY EFFECTS**

1528   Preclude (Preempt), Impede (Exert), Expose (Detect)

1529   **REFERENCES**

1530   Source Control: CA-07(04)

1531   **03.12.04E Internal System Connections**

1532   a. Authorize internal connections of [Assignment: organization-defined system
1533   components or classes of components] to the system.

1534   b. Document, for each internal connection, the interface characteristics, security
1535   requirements, and the nature of the information communicated.

1536
1537
   c. Terminate internal system connections after [Assignment: organization-defined conditions].

1538
1539
   d. Review [Assignment: organization-defined frequency] the continued need for each internal connection.

1540 **DISCUSSION**

1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
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.

1553 **PROTECTION STRATEGY**

1554 PRA

1555 **ADVERSARY EFFECTS**

1556 Preclude (Preempt), Impede (Exert)

1557 **REFERENCES**

1558 Source Control: CA-09

1559 **3.13. System and Communications Protection**

1560 **03.13.01E Heterogeneity**

1561
1562
1563
Use a diverse set of information technologies for the following system components in the implementation of the system: [*Assignment: organization-defined system components*].

1564 **DISCUSSION**

1565
1566
1567
1568
1569
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

1570 against other system components, further increasing the adversary work factor to
1571 successfully complete planned attacks. An increase in diversity may add complexity
1572 and management overhead that could ultimately lead to mistakes and unauthorized
1573 configurations.

1574 **PROTECTION STRATEGY**

1575 PRA, CRS

1576 **ADVERSARY EFFECTS**

1577 Preclude (Preempt), Impede (Contain, Exert), Limit (Reduce)

1578 **REFERENCES**

1579 Source Control: SC-29

1580 **03.13.02E Randomness**

1581 Use the following techniques to introduce randomness into organizational
1582 operations and assets: [*Assignment: organization-defined techniques*].

1583 **DISCUSSION**

1584 Randomness introduces increased levels of uncertainty for adversaries regarding the
1585 actions that organizations take to defend their systems against attacks. Such actions
1586 may impede the ability of adversaries to correctly target organizational systems that
1587 support critical missions or business functions. Uncertainty may cause adversaries to
1588 hesitate before initiating or continuing attacks. Misdirection techniques that involve
1589 randomness include performing certain routine actions at different times of day,
1590 employing different information technologies, using different suppliers, and rotating
1591 the roles and responsibilities of organizational personnel.

1592 **PROTECTION STRATEGY**

1593 PRA, CRS

1594 **ADVERSARY EFFECTS**

1595 Preclude (Preempt), Impede (Exert), Redirect (Deceive)

1596 **REFERENCES**

1597 Source Control: SC-30(02)

1598 **03.13.03E Concealment and Misdirection**

1599   Use the following concealment and misdirection techniques to confuse and mislead
1600   adversaries: [*Assignment: organization-defined concealment and misdirection*
1601   *techniques*].

1602   **DISCUSSION**

1603   Concealment and misdirection techniques can significantly reduce the targeting
1604   capabilities of adversaries (i.e., window of opportunity and available attack surface)
1605   to initiate and complete attacks. For example, virtualization techniques provide
1606   organizations with the ability to disguise systems, potentially reducing the likelihood
1607   of successful attacks without the cost of having multiple platforms. The increased
1608   use of specific concealment and misdirection techniques and methods, including
1609   randomness, uncertainty, and virtualization, may sufficiently confuse and mislead
1610   adversaries and subsequently increase the risk of discovery or exposing tradecraft.
1611   Concealment and misdirection techniques may provide additional time to perform
1612   core mission and business functions. The implementation of concealment and
1613   misdirection techniques may add to the complexity and management overhead
1614   required for the system.

1615   **PROTECTION STRATEGY**

1616   PRA, CRS

1617   **ADVERSARY EFFECTS**

1618   Preclude (Preempt), Impede (Exert), Redirect (Deceive)

1619   **REFERENCES**

1620   Source Control: SC-30

1621 **03.13.04E Isolation of System Components**

1622   Implement boundary protection mechanisms to isolate [*Assignment: organization-*
1623   *defined system components*].

1624   **DISCUSSION**

1625   Organizations can isolate system components that perform different mission or
1626   business functions. Isolating system components with boundary protection
1627   mechanisms allows for the increased protection of individual system components
1628   and more effective control of information flows between those components.
1629   Isolating system components provides enhanced protection that limits the potential
1630   harm of hostile cyber-attacks and errors. The degree of isolation varies depending
1631   on the mechanisms selected. Boundary protection mechanisms include routers,
1632   gateways, and firewalls that separate system components into physically separate

1633   networks or subnetworks; cross-domain devices that separate subnetworks;
1634   virtualization techniques; and the encryption of information flows among system
1635   components using distinct encryption keys. This requirement enhances SP 800-171
1636   requirement 03.13.01.

1637   **PROTECTION STRATEGY**

1638   PRA

1639   **ADVERSARY EFFECTS**

1640   Preclude (Preempt), Impede (Exert), Limit (Reduce)

1641   **REFERENCES**

1642   Source Control: SC-07(21)

1643   **03.13.05E Change Processing and Storage Locations**

1644   Change the location of [*Assignment: organization-defined processing and/or
1645   storage*] [*Selection (one):* [*Assignment: organization-defined time frequency*]*; at
1646   random time intervals*].

1647   **DISCUSSION**

1648   Adversaries target critical missions and business functions and the systems that
1649   support those missions and business functions while also trying to minimize the
1650   exposure of their existence and tradecraft. The homogeneous, deterministic, and
1651   static nature of organizational systems targeted by adversaries make such systems
1652   more susceptible to attacks with less adversary cost and effort to be successful.
1653   Changing processing and storage locations (also referred to as moving target
1654   defense) addresses the advanced persistent threat using techniques such as
1655   virtualization, distributed processing, and replication. This enables organizations to
1656   relocate the system components (i.e., processing, storage) that support critical
1657   missions and business functions. Changing the locations of processing activities
1658   and/or storage sites introduces a degree of uncertainty to the targeting activities of
1659   adversaries. The targeting uncertainty increases the work factor of adversaries and
1660   makes compromises or breaches of the organizational systems more difficult and
1661   time-consuming. Uncertainty also increases the chances that adversaries may
1662   inadvertently disclose certain aspects of their tradecraft while attempting to locate
1663   critical organizational assets.

1664   **PROTECTION STRATEGY**

1665   CRS

1666   **ADVERSARY EFFECTS**

1667   Preclude (Preempt, Negate), Impede (Contain, Exert), Limit (Reduce)

1668   **REFERENCES**

1669   Source Control: SC-30(3)

1670   **03.13.06E Platform-Independent Applications**

1671   Implement the following platform-independent applications within organizational
1672   systems: [*Assignment: organization-defined platform-independent applications*].

1673   **DISCUSSION**

1674   Platforms are the hardware, software, and firmware components used to execute
1675   the organization's software applications. Platforms include operating systems, the
1676   underlying computer architectures, or both. Platform-independent applications are
1677   applications with the capability to execute on multiple platforms. Such applications
1678   promote portability and reconstitution on different platforms. The portability of
1679   applications and the ability to reconstitute applications on different platforms
1680   increase the availability of mission-essential functions within organizations when
1681   systems with specific operating systems are under attack.

1682   **PROTECTION STRATEGY**

1683   CRS

1684   **ADVERSARY EFFECTS**

1685   Limit (Shorten, Reduce)

1686   **REFERENCES**

1687   Source Control: SC-27

1688   **03.13.07E Virtualization Techniques**

1689   Use virtualization techniques to support the deployment of a diversity of operating
1690   systems and applications that are changed [*Assignment: organization-defined
1691   frequency*].

1692   **DISCUSSION**

1693   While frequent changes to operating systems and applications can pose significant
1694   configuration management challenges, the changes can result in an increased work
1695   factor for adversaries to conduct successful attacks. Changing virtual operating
1696   systems or applications, as opposed to changing actual operating systems or
1697   applications, provides virtual changes that impede attacker success while reducing

1698 configuration management efforts. Virtualization techniques can assist in isolating
1699 untrustworthy software or software of dubious provenance into confined execution
1700 environments.

1701 **PROTECTION STRATEGY**

1702 PRA, CRS

1703 **ADVERSARY EFFECTS**

1704 Preclude (Preempt), Impede (Exert), Limit (Reduce)

1705 **REFERENCES**

1706 Source Control: SC-29(01)

1707 **03.13.08E Decoys**

1708 Use components within organizational systems specifically designed to be the target
1709 of malicious attacks for detecting, deflecting, and analyzing such attacks.

1710 **DISCUSSION**

1711 Decoys (i.e., honeypots, honeynets, or deception nets) are established to attract
1712 adversaries and deflect attacks away from the operational systems that support
1713 organizational missions and business functions. The use of decoys requires some
1714 supporting isolation measures to ensure that any deflected malicious code does not
1715 infect organizational systems.

1716 **PROTECTION STRATEGY**

1717 DLO, CRS

1718 **ADVERSARY EFFECTS**

1719 Expose (Detect), Limit (Reduce)

1720 **REFERENCES**

1721 Source Control: SC-26

1722 **03.13.09E Security Tool, Mechanism, and Support Component Isolation**

1723 Isolate [*Assignment: organization-defined information security tools, mechanisms,*
1724 *and support components*] from other internal system components by implementing
1725 physically separate subnetworks with managed interfaces to other components of
1726 the system.

1727　**DISCUSSION**

1728　Physically separate subnetworks with managed interfaces are useful for isolating
1729　computer network defenses from critical operational processing networks to
1730　prevent adversaries from discovering the analysis and forensics techniques
1731　employed by organizations. This requirement enhances SP 800-171 requirement
1732　03.13.01.

1733　**PROTECTION STRATEGY**

1734　PRA

1735　**ADVERSARY EFFECTS**

1736　Preclude (Preempt), Impede (Exert)

1737　**REFERENCES**

1738　Source Control: SC-07(13)

1739　**03.13.10E　Separate Subnetworks**

1740　Implement separate network addresses to connect to systems in different security
1741　domains.

1742　**DISCUSSION**

1743　The decomposition of systems into subnetworks (i.e., subnets) helps to provide the
1744　appropriate level of protection for network connections to security domains that
1745　contain information with different sensitivity levels. This requirement enhances SP
1746　800-171 requirement 03.13.01.

1747　**PROTECTION STRATEGY**

1748　PRA

1749　**ADVERSARY EFFECTS**

1750　Preclude (Preempt), Impede (Exert), Limit (Reduce)

1751　**REFERENCES**

1752　Source Control: SC-07(22)

1753　**03.13.11E　Thin Nodes**

1754　Implement minimal functionality and information storage on the following system
1755　components: [*Assignment: organization-defined system components*].

1756   **DISCUSSION**

1757   The deployment of system components with minimal functionality reduces the need
1758   to secure every endpoint and may reduce the exposure of information, systems, and
1759   services to attacks. Reduced or minimal functionality includes diskless nodes and
1760   thin client technologies.

1761   **PROTECTION STRATEGY**

1762   PRA

1763   **ADVERSARY EFFECTS**

1764   Preclude (Preempt), Impede (Contain)

1765   **REFERENCES**

1766   Source Control: SC-25

1767   **03.13.12E Denial-of-Service Protection**

1768   a. [Selection (one): Protect against; Limit] the effects of the following types of
1769   denial-of-service events: [Assignment: organization-defined types of denial-of-
1770   service events].

1771   b. Implement the following safeguards to achieve the denial-of-service
1772   [Assignment: organization-defined safeguards by type of denial-of-service
1773   event].

1774   **DISCUSSION**

1775   Denial-of-service events may occur due to a variety of internal and external causes,
1776   such as an attack by an adversary or a lack of planning to support organizational
1777   needs with respect to capacity and bandwidth. Cyber-attacks can occur across a
1778   wide range of network protocols (e.g., IPv4, IPv6). A variety of technologies are
1779   available to limit or eliminate the origination and effects of denial-of-service events.
1780   For example, boundary protection devices can filter certain types of packets to
1781   protect system components on internal networks from being directly affected by or
1782   the source of denial-of-service attacks. Employing increased network capacity and
1783   bandwidth combined with service redundancy also reduces the susceptibility to
1784   denial-of-service events.

1785   **PROTECTION STRATEGY**

1786   PRA, CRS

1787   **ADVERSARY EFFECTS**

1788   Preclude (Preempt, Negate), Impede (Exert), Limit (Reduce)

1789   **REFERENCES**

1790   Source Control: SC-05

1791   **03.13.13E Port and Input/Output Device Access**

1792   [*Selection (one): Physically; Logically*] disable or remove [*Assignment: organization-*
1793   *defined connection ports or input/output devices*] on the following systems or
1794   system components: [*Assignment: organization-defined systems or system*
1795   *components*].

1796   **DISCUSSION**

1797   Connection ports include Universal Serial Bus (USB), Thunderbolt, and Firewire (IEEE
1798   1394). Input/output (I/O) devices include compact disc and digital versatile disc
1799   drives. Disabling or removing such connection ports and I/O devices helps prevent
1800   the exfiltration of information from systems and the introduction of malicious code
1801   from those ports or devices. Physically disabling or removing ports and/or devices is
1802   the stronger action.

1803   **PROTECTION STRATEGY**

1804   PRA

1805   **ADVERSARY EFFECTS**

1806   Preclude (Preempt), Impede (Contain)

1807   **REFERENCES**

1808   Source Control: SC-41

1809   **03.13.14E Detonation Chambers**

1810   Implement a detonation chamber capability within [*Assignment: organization-*
1811   *defined system, system component, or location*].

1812   **DISCUSSION**

1813   Detonation chambers (also known as dynamic execution environments) allow
1814   organizations to open email attachments, execute untrusted or suspicious
1815   applications, and execute URL requests in the safety of an isolated environment or a
1816   virtualized sandbox. Protected and isolated execution environments provide a
1817   means of determining whether the associated attachments or applications contain
1818   malicious code. While related to the concept of deception nets, the employment of
1819   detonation chambers is not intended to maintain a long-term environment in which
1820   adversaries can operate and their actions can be observed. Rather, detonation
1821   chambers are intended to quickly identify malicious code and reduce the likelihood

1822   that the code is propagated to user environments of operation or prevent such
1823   propagation completely.

1824   **PROTECTION STRATEGY**

1825   PRA, DLO

1826   **ADVERSARY EFFECTS**

1827   Preclude (Preempt), Negate), Impede (Contain, Exert), Expose (Detect, Reveal)

1828   **REFERENCES**

1829   Source Control: SC-44

1830   **3.14. System and Information Integrity**

1831   **03.14.01E Software, Firmware, and Information Integrity**

1832   a. Use integrity verification tools to detect unauthorized changes to the following
1833   software, firmware, and information: [*Assignment: organization-defined*
1834   *software, firmware, and information*].

1835   b. Take the following actions when unauthorized changes to the software,
1836   firmware, and information are detected: [*Assignment: organization-defined*
1837   *actions*].

1838   **DISCUSSION**

1839   Unauthorized changes to software, firmware, and information can occur due to
1840   errors or malicious activity. Software includes boot firmware, operating systems
1841   with key internal components (e.g., kernels or drivers), middleware, and
1842   applications. Firmware interfaces include Unified Extensible Firmware Interface
1843   (UEFI) and Basic Input/Output Systems (BIOS). Information includes CUI and
1844   metadata that contains security attributes associated with information. Integrity-
1845   checking mechanisms—including parity checks, cyclical redundancy checks,
1846   cryptographic hashes, and associated tools—can automatically monitor the integrity
1847   of systems and hosted applications.

1848   Verifying the integrity of the organization's security-critical or essential software is
1849   an important capability since corrupted software is the primary attack vector used
1850   by adversaries to undermine or disrupt the proper functioning of organizational
1851   systems. This capability helps system components protect the integrity of boot
1852   firmware in organizational systems by verifying the integrity and authenticity of
1853   updates to the firmware prior to applying changes to the system component and
1854   preventing unauthorized processes from modifying the boot firmware. There are
1855   many ways to verify software integrity throughout the system development life

1856   cycle. Root of trust mechanisms (e.g., secure boot, trusted platform modules, UEFI)
1857   verify that only trusted code is executed during boot processes. The employment of
1858   cryptographic signatures ensures the integrity and authenticity of critical software
1859   that stores, processes, or transmits, CUI. Cryptographic signatures include digital
1860   signatures and the computation and application of signed hashes using asymmetric
1861   cryptography, protecting the confidentiality of the key used to generate the hash,
1862   and using the public key to verify the hash information. Hardware roots of trust are
1863   considered to be more secure.

1864   **PROTECTION STRATEGY**

1865   PRA, DLO

1866   **ADVERSARY EFFECTS**

1867   Preclude (Preempt), Expose (Detect)

1868   **REFERENCES**

1869   Source Control: SI-07

1870   **03.14.02E Withdrawn**

1871   Addressed by 03.14.06.

1872   **03.14.03E Withdrawn**

1873   Addressed by 03.15.01E, 03.13.01, and 03.16.01.

1874   **03.14.04E Refresh from Trusted Sources**

1875   Obtain software and data employed during system component and service refreshes
1876   from the following trusted sources: [*Assignment: organization-defined trusted*
1877   *sources*].

1878   **DISCUSSION**

1879   Trusted sources include software and data from write-once, read-only media or
1880   from selected offline secure storage facilities.

1881   **PROTECTION STRATEGY**

1882   PRA

1883   **ADVERSARY EFFECTS**

1884   Preclude (Preempt), Impede (Exert)

1885   **REFERENCES**

1886   Source Control: SI-14(01)

1887   **03.14.05E Non-Persistent Information**

1888   a.   [*Selection (one): Refresh* [*Assignment: organization-defined information*]
1889   [*Assignment: organization-defined frequency*]*; Generate* [*Assignment:*
1890   *organization-defined information*] *on demand*].

1891   b.   Delete information when no longer needed.

1892   **DISCUSSION**

1893   Retaining unneeded information makes that information a potential target for
1894   advanced adversaries searching for high value assets to compromise through
1895   unauthorized disclosure, unauthorized modification, or exfiltration. For system-
1896   related information, unnecessary retention provides advanced adversaries
1897   information that can assist in their reconnaissance and lateral movement through
1898   the system.

1899   **PROTECTION STRATEGY**

1900   PRA

1901   **ADVERSARY EFFECTS**

1902   Preclude (Preempt), Impede (Exert)

1903   **REFERENCES**

1904   Source Control: SI-14(02)

1905   **03.14.06E Withdrawn**

1906   Addressed by 03.11.02E and 03.11.09E.

1907   **03.14.07E Withdrawn**

1908   Addressed by 03.14.08E, 03.14.10E, 03.14.14E, 03.17.03E, 03.16.01.

1909   **03.14.08E Integrity Checks**

1910   Perform an integrity check of [*Assignment: organization-defined software, firmware,*
1911   *and information*] [*Selection (one or more): at startup; at* [*Assignment: organization-*
1912   *defined transitional states or security-relevant events*]; [*Assignment: organization-*
1913   *defined frequency*]].

1914 **DISCUSSION**

1915 Security-relevant events include the identification of new threats to which systems
1916 are susceptible and the installation of hardware, software, or firmware. Transitional
1917 states include system startup, restart, shutdown, and abort.

1918 **PROTECTION STRATEGY**

1919 PRA

1920 **ADVERSARY EFFECTS**

1921 Preclude (Preempt), Impede (Exert)

1922 **REFERENCES**

1923 Source Control: SI-07(01)

1924 **03.14.09E Cryptographic Protection**

1925 Implement cryptographic mechanisms to detect unauthorized changes to software,
1926 firmware, and information.

1927 **DISCUSSION**

1928 Cryptographic mechanisms used to protect integrity include digital signatures and
1929 the computation and application of signed hashes using asymmetric cryptography,
1930 protecting the confidentiality of the key used to generate the hash, and using the
1931 public key to verify the hash information. Organizations that employ cryptographic
1932 mechanisms also consider cryptographic key management solutions.

1933 **PROTECTION STRATEGY**

1934 PRA, DLO

1935 **ADVERSARY EFFECTS**

1936 Preclude (Preempt), Impede (Exert), Expose (Detect)

1937 **REFERENCES**

1938 Source Control: SI-07(06)

1939 **03.14.10E Protection of Boot Firmware**

1940 Implement the following mechanisms to protect the integrity of boot firmware in
1941 [*Assignment: organization-defined system components*]: [*Assignment: organization-*
1942 *defined mechanisms*].

1943　**DISCUSSION**

1944　Unauthorized modifications to boot firmware may indicate a sophisticated, targeted
1945　attack. These types of targeted attacks can result in a permanent denial of service or
1946　a persistent malicious code presence. These situations can occur if the firmware is
1947　corrupted or if the malicious code is embedded within the firmware. System
1948　components can protect the integrity of boot firmware in organizational systems by
1949　verifying the integrity and authenticity of updates to the firmware prior to applying
1950　changes to the system component and preventing unauthorized processes from
1951　modifying the boot firmware.

1952　**PROTECTION STRATEGY**

1953　PRA

1954　**ADVERSARY EFFECTS**

1955　Preclude (Preempt), Impede (Exert)

1956　**REFERENCES**

1957　Source Control: SI-07(10)

1958　**03.14.11E　Integration of Detection and Response Capability**

1959　Incorporate the detection of the following unauthorized changes into the
1960　organizational incident response capability: [*Assignment: organization-defined*
1961　*security-relevant changes to the system*].

1962　**DISCUSSION**

1963　Integrating a detection and response capability ensures that detected events are
1964　tracked, monitored, corrected, and available for historical purposes. Maintaining
1965　historical records is important to identify and discern adversary actions over an
1966　extended time period and for possible legal actions. Security-relevant changes
1967　include unauthorized changes to established configuration settings or the
1968　unauthorized elevation of system privileges.

1969　**PROTECTION STRATEGY**

1970　DLO

1971　**ADVERSARY EFFECTS**

1972　Expose (Detect)

1973　**REFERENCES**

1974　Source Control: SI-07(07)

1975 **03.14.12E Information Input Validation**

1976   Check the validity of the following information inputs: [*Assignment: organization-*
1977   *defined information inputs to the system*].

1978   **DISCUSSION**

1979   Checking the valid syntax and semantics of system inputs—including character set,
1980   length, numerical range, and acceptable values—verifies that inputs match specified
1981   definitions for format and content. For example, if the organization specifies that
1982   numerical values between 1-100 are the only acceptable inputs for a field in a given
1983   application, inputs of "387," "abc," or "%K%" are invalid and not accepted as inputs
1984   to the system. Valid inputs are likely to vary from field to field within a software
1985   application. Applications typically follow well-defined protocols that use structured
1986   messages (i.e., commands or queries) to communicate between software modules
1987   or system components.

1988   Structured messages can contain raw or unstructured data interspersed with
1989   metadata or control information. If software applications use attacker-supplied
1990   inputs to construct structured messages without properly encoding such messages,
1991   then the attacker could insert malicious commands or special characters that can
1992   cause the data to be interpreted as control information or metadata. Consequently,
1993   the module or component that receives the corrupted output will perform the
1994   wrong operations or otherwise interpret the data incorrectly. Prescreening inputs
1995   prior to passing them to interpreters prevents content from being unintentionally
1996   interpreted as commands. Input validation ensures accurate and correct inputs and
1997   prevents attacks, such as cross-site scripting and a variety of injection attacks.

1998   **PROTECTION STRATEGY**

1999   PRA

2000   **ADVERSARY EFFECTS**

2001   Preclude (Preempt)

2002   **REFERENCES**

2003   Source Control: SI-10

2004 **03.14.13E Error Handling**

2005   a. Generate error messages that provide information necessary for corrective
2006   actions without revealing information that could be exploited.

2007   b. Reveal error messages only to [*Assignment: organization-defined personnel or*
2008   *roles*].

2009	**DISCUSSION**

2010	Organizations consider the structure and content of error messages. The extent to
2011	which systems can handle error conditions is guided and informed by organizational
2012	policy and operational requirements. Exploitable information includes stack traces
2013	and implementation details; erroneous logon attempts with passwords mistakenly
2014	entered as the username; mission or business information that can be derived from,
2015	if not stated explicitly by, the information recorded; and personally identifiable
2016	information, such as account numbers, Social Security numbers, and credit card
2017	numbers. Error messages may also provide a covert channel for transmitting
2018	information.

2019	**PROTECTION STRATEGY**

2020	PRA

2021	**ADVERSARY EFFECTS**

2022	Preclude (Preempt)

2023	**REFERENCES**

2024	Source Control: SI-11

2025	**03.14.14E Memory Protection**

2026	Implement the following safeguards to protect the system memory from
2027	unauthorized code execution: [*Assignment: organization-defined safeguards*].

2028	**DISCUSSION**

2029	Some adversaries launch attacks with the intent of executing code in non-executable
2030	regions of memory or in memory locations that are prohibited. The safeguards used
2031	to protect memory include data execution prevention and address space layout
2032	randomization (ASLR). Data execution prevention safeguards can be hardware- or
2033	software-enforced with hardware enforcement providing the greater strength of
2034	mechanism.

2035	**PROTECTION STRATEGY**

2036	PRA

2037	**ADVERSARY EFFECTS**

2038	Preclude (Preempt), Impede (Exert)

2039	**REFERENCES**

2040	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

2076   **03.14.16E Tainting**

2077   Embed data or capabilities in the following systems or system components to
2078   determine if organizational data has been exfiltrated or improperly removed from
2079   the organization: [*Assignment: organization-defined systems or system components*].

2080   **DISCUSSION**

2081   Many cyber-attacks target organizational information or information that the
2082   organization holds on behalf of other entities with the intent to exfiltrate that
2083   information. In addition, insider attacks and erroneous user procedures can remove
2084   information from the system in violation of organizational policies. Tainting
2085   approaches can range from passive to active. A passive tainting approach can be as
2086   simple as adding false email names and addresses to an internal database. If the
2087   organization receives email at one of the false email addresses, it knows that the
2088   database has been compromised. Moreover, the organization knows that the email
2089   was sent by an unauthorized entity, so any packets it includes potentially contain
2090   malicious code, and the unauthorized entity may have potentially obtained a copy of
2091   the database. Another tainting approach includes embedding false data or
2092   steganographic data in files to enable the data to be found via open-source analysis.
2093   An active tainting approach can include embedding software in the data that is able
2094   to "call home," thereby alerting the organization to its capture and possibly its
2095   location and the path by which it was exfiltrated or removed.

2096   **PROTECTION STRATEGY**

2097   DLO

2098   **ADVERSARY EFFECTS**

2099   Expose (Detect)

2100   **REFERENCES**

2101   Source Control: SI-20

2102   **03.14.17E System-Generated Alerts**

2103   Alert [*Assignment: organization-defined personnel or roles*] when the following
2104   system-generated indications of compromise or potential compromise occur:
2105   [*Assignment: organization-defined compromise indicators*].

2106   **DISCUSSION**

2107   Alerts may be generated from a variety of sources, including audit records or inputs
2108   from malicious code protection mechanisms, intrusion detection or prevention
2109   mechanisms, or boundary protection devices such as firewalls, gateways, and
2110   routers. Alerts can be automated and transmitted telephonically, by electronic mail

2111   messages, or by text messaging. Organizational personnel on the alert notification
2112   list can include system administrators, mission or business owners, system owners,
2113   information owners or stewards, chief information security officers, and system
2114   security officers. In contrast to alerts generated by the system, alerts generated by
2115   the organization focuses on information sources external to the system, such as
2116   suspicious activity reports and reports on potential insider threats. This requirement
2117   enhances SP 800-171 requirement 03.14.06.

2118   **PROTECTION STRATEGY**

2119   DLO

2120   **ADVERSARY EFFECTS**

2121   Expose (Detect)

2122   **REFERENCES**

2123   Source Controls: SI-04(05)

2124   **03.14.18E Automated Organization-Generated Alerts**

2125   Alert [*Assignment: organization-defined personnel or roles*] using [*Assignment:*
2126   *organization-defined automated mechanisms*] when the following indications of
2127   inappropriate or unusual activities with security implications occur: [*Assignment:*
2128   *organization-defined activities that trigger alerts*].

2129   **DISCUSSION**

2130   The sources for organization-generated alerts are focused on entities such as
2131   suspicious activity reports and reports on potential insider threats. Organizational
2132   personnel on the system alert notification list include system administrators, mission
2133   or business owners, system owners, chief information security officers, and system
2134   security officers. In contrast to the alerts generated by the organization, alerts
2135   generated by the system focus on information sources that are internal to the
2136   system, such as audit records. This requirement enhances SP 800-171 requirement
2137   03.14.06.

2138   **PROTECTION STRATEGY**

2139   DLO

2140   **ADVERSARY EFFECTS**

2141   Expose (Detect)

2142   **REFERENCES**

2143   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].

2179   **PROTECTION STRATEGY**

2180   PRA

2181   **ADVERSARY EFFECTS**

2182   Preclude (Preempt), Impede (Exert)

2183   **REFERENCES**

2184   Source Control: [PL-08](#)

2185   **03.15.02E Defense In Depth**

2186   a. Design the security architecture for the system using a defense-in-depth
2187   approach.

2188   b. Allocate [*Assignment: organization-defined security requirements*] to
2189   [*Assignment: organization-defined architectural layers and locations*].

2190   c. Ensure that the allocated requirements operate in a coordinated and mutually
2191   reinforcing manner.

2192   **DISCUSSION**

2193   Organizations strategically allocate security requirements and the associated
2194   protection mechanisms in the security architecture so that adversaries must
2195   overcome multiple defensive layers to achieve their objective. Requiring adversaries
2196   to defeat multiple defensive layers makes it more difficult to attack systems by
2197   increasing the work factor of the adversary. It also increases the likelihood of
2198   detection. Defense-in-depth architectural approaches include modularity and
2199   layering, the separation of system and user functionality, and security function
2200   isolation.

2201   The coordination of allocated security requirements is essential to help ensure that
2202   an attack that involves one requirement does not create adverse, unintended
2203   consequences (e.g., system lockout and cascading alarms) by interfering with other
2204   requirements. The value of organizational assets and the impacts or consequences
2205   of loss are important considerations in providing additional defensive layers.

2206   **PROTECTION STRATEGY**

2207   PRA, CRS

2208   **ADVERSARY EFFECTS**

2209   Preclude (Preempt), Impede (Exert), Limit (Reduce)

2210   **REFERENCES**

2211   Source Control: PL-08(01)

2212   **03.15.03E Supplier Diversity**

2213   Require that [*Assignment: organization-defined safeguards*] allocated to
2214   [*Assignment: organization-defined locations and architectural layers*] are obtained
2215   from different suppliers.

2216   **DISCUSSION**

2217   Information technology security products have different strengths and weaknesses.
2218   Providing a broad spectrum of products complements the individual offerings. For
2219   example, vendors that offer malicious code protection typically update their
2220   products at different times and develop solutions for known viruses, Trojans, or
2221   worms based on their priorities and development schedules. Deploying different
2222   types of products at different locations increases the likelihood that at least one of
2223   the products will detect the malicious code.

2224   **PROTECTION STRATEGY**

2225   PRA, CRS

2226   **ADVERSARY EFFECTS**

2227   Preclude (Preempt, Negate), Impede (Exert), Limit (Reduce)

2228   **REFERENCES**

2229   Source Control: PL-08(02)

2230   **3.16. System and Services Acquisition**

2231   **03.16.01E Specialization**

2232   Implement [*Selection (one or more): design; modification; augmentation;
2233   reconfiguration*] on [*Assignment: organization-defined systems or system
2234   components*] supporting mission-essential services or functions to increase the
2235   trustworthiness in those systems or components.

2236   **DISCUSSION**

2237   Systems or system components that support mission-essential services or functions
2238   must often be enhanced to maximize the trustworthiness of the resource.
2239   Sometimes, this enhancement is done at the design level. In other instances, it is
2240   done post-design, either through modifications of the system in question or by
2241   augmenting the system with additional components. For example, supplemental

2242   authentication or non-repudiation functions may be added to the system to enhance
2243   critical resources that depend on the organization-defined resources.

2244   **PROTECTION STRATEGY**

2245   PRA

2246   **ADVERSARY EFFECTS**

2247   Preclude (Preempt), Impede (Exert)

2248   **REFERENCES**

2249   Source Control: SA-23

2250   ## 3.17. Supply Chain Risk Management

2251   **03.17.01E Notification Agreements**

2252   Establish agreements and procedures with entities involved in the supply chain for
2253   the system, system component, or system service regarding the [*Selection (one or*
2254   *more): notification of supply chain compromises; results of assessments or audits;*
2255   *provision of* [*Assignment: organization-defined information*]].

2256   **DISCUSSION**

2257   Establishing agreements and procedures facilitates communications among supply
2258   chain entities. Early notification of compromises and potential compromises in the
2259   supply chain that may adversely affect or have adversely affected organizational
2260   systems or system components is essential for organizations to effectively respond
2261   to such incidents. The results of assessments or audits may include open-source
2262   information that contributed to a decision or result and could be used to help the
2263   supply chain entity resolve a concern or improve its processes.

2264   **PROTECTION STRATEGY**

2265   DLO

2266   **ADVERSARY EFFECTS**

2267   Expose (Detect), Limit (Shorten, Reduce)

2268   **REFERENCES**

2269   Source Control: SR-08

2270   **03.17.02E Inspection of Systems or Components**

2271   Inspect the following systems or system components [*Selection (one or more): at
2272   random;* [*Assignment: organization-defined frequency*]*; upon* [*Assignment:
2273   organization-defined indications of need for inspection*]] to detect tampering:
2274   [*Assignment: organization-defined systems or system components*].

2275   **DISCUSSION**

2276   Inspecting systems or systems components for tamper resistance and detection
2277   addresses physical and logical tampering and is applied to systems and system
2278   components that are removed from organization-controlled areas. Indications of a
2279   need for inspection include changes in packaging, specifications, factory location, or
2280   entity in which the part is purchased and when individuals return from travel to
2281   high-risk locations.

2282   **PROTECTION STRATEGY**

2283   DLO

2284   **ADVERSARY EFFECTS**

2285   Expose (Detect)

2286   **REFERENCES**

2287   Source Control: [SR-10](#)

2288   **03.17.03E Component Authenticity**

2289   a. Develop and implement anti-counterfeit policy and procedures that include the
2290   means to detect and prevent counterfeit components from entering the system.

2291   b. Report counterfeit system components to [*Selection (one or more): source of
2292   counterfeit component;* [*Assignment: organization-defined external reporting
2293   organizations*]*;* [*Assignment: organization-defined personnel or roles*]].

2294   **DISCUSSION**

2295   Sources of counterfeit components include manufacturers, developers, vendors, and
2296   contractors. Anti-counterfeiting policies and procedures support tamper resistance
2297   and provide a level of protection against the introduction of malicious code. External
2298   reporting organizations include the Cybersecurity and Infrastructure Security Agency
2299   (CISA).

2300   **PROTECTION STRATEGY**

2301   PRA, DLO

2302   **ADVERSARY EFFECTS**

2303   Preclude (Preempt), Expose (Detect)

2304   **REFERENCES**

2305   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

2346 [13] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber-Resilient
2347   Systems: A Systems Security Engineering Approach. (National Institute of Standards and
2348   Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v2r1.
2349   https://doi.org/10.6028/NIST.SP.800-160v2r1

2350 [14] Johnson CS, Waltermire DA, Badger ML, Skorupka C, Snyder J (2016) Guide to Cyber Threat
2351   Information Sharing. (National Institute of Standards and Technology, Gaithersburg, MD),
2352   NIST Special Publication (SP) NIST SP 800-150.
2353   https://doi.org/10.6028/NIST.SP.800-150

2354 [15] Joint Task Force Transformation Initiative (2022) Assessing Security and Privacy Controls in
2355   Information Systems and Organizations. (National Institute of Standards and Technology,
2356   Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53Ar5.
2357   https://doi.org/10.6028/NIST.SP.800-53Ar5

2358 [16] Committee on National Security Systems (2022) Committee on National Security Systems
2359   (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction
2360   4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

2361 [17] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk:
2362   Organization, Mission, and Information System View. (National Institute of Standards and
2363   Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-39.
2364   https://doi.org/10.6028/NIST.SP.800-39

2365 [18] Office of Management and Budget Circular A-130, Managing Information as a Strategic
2366   Resource, July 2016. Available at https://www.whitehouse.gov/wp-
2367   content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

2368 [19] U.S. Government Accountability Office (2018) Weapons Systems Cybersecurity: DOD Just
2369   Beginning to Grapple with Scale of Vulnerabilities. (GAO, Washington, DC), Report to the
2370   Committee on Armed Services, U.S. Senate, GAO 19-128. Available at
2371   https://www.gao.gov/assets/700/694913.pdf

2372 [20] Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed. Available at
2373   https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-
2374   subchapII-sec3552

2375 [21] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments.
2376   (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2377   Publication (SP) NIST SP 800-30r1.
2378   https://doi.org/10.6028/NIST.SP.800-30r1

2379 [22] Ross R, Winstead M, McEvilley M (2022) Engineering Trustworthy Secure Systems.
2380   (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
2381   Publication (SP) NIST SP 800-160v1r1. https://doi.org/10.6028/NIST.SP.800-160v1r1

2382 [23] Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards.
2383   2017 ed. Available at https://www.govinfo.gov/app/details/USCODE-2017-
2384   title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331

2385 [24] Title 44 U.S. Code, Sec. 3502, Definitions. 2017 ed. Available at
2386   https://www.govinfo.gov/app/details/USCODE-2021-title44/USCODE-2021-title44-chap35-
2387   subchapI-sec3502

2388   [25] National Institute of Standards and Technology (2019) Roots of Trust Project. Available at
2389   https://csrc.nist.gov/projects/hardware-roots-of-trust

2390   [26] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused
2391   Configuration Management of Information Systems. (National Institute of Standards and
2392   Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-128, Includes
2393   updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128

2394   **Appendix A. Acronyms**

2395   **APT**
2396   Advanced Persistent Threat

2397   **ASLR**
2398   Address Space Layout Randomization

2399   **BIOS**
2400   Basic Input/Output System

2401   **CERT**
2402   Computer Emergency Response Team

2403   **CERTCC**
2404   CERT Coordination Center

2405   **CFR**
2406   Code of Federal Regulations

2407   **CIRT**
2408   Cyber Incident Response Team

2409   **CISA**
2410   Cybersecurity and Infrastructure Security Agency

2411   **CNSS**
2412   Committee on National Security Systems

2413   **CRS**
2414   Cyber Resiliency

2415   **CUI**
2416   Controlled Unclassified Information

2417   **DIB**
2418   Defense Industrial Base

2419   **DIB CS**
2420   Defense Industrial Base Cybersecurity Sharing

2421   **DLO**
2422   Damage-Limiting Operations

2423   **EO**
2424   Executive Order

2425   **FIPS**
2426   Federal Information Processing Standards

2427   **FIRST**
2428   Forum of Incident Response and Security Teams

2429   **FISMA**
2430   Federal Information Security Modernization Act

2431 **FOIA**
2432 Freedom of Information Act

2433 **GAO**
2434 Government Accountability Office

2435 **HVA**
2436 High Value Asset

2437 **IIoT**
2438 Industrial Internet of Things

2439 **IoT**
2440 Internet of Things

2441 **ISAC**
2442 Information Sharing and Analysis Centers

2443 **ISAO**
2444 Information Sharing and Analysis Organizations

2445 **ISOO**
2446 Information Security Oversight Office

2447 **IT**
2448 Information Technology

2449 **ITL**
2450 Information Technology Laboratory

2451 **NARA**
2452 National Archives and Records Administration

2453 **NIST**
2454 National Institute of Standards and Technology

2455 **NIST IR**
2456 NIST Interagency or Internal Report

2457 **ODP**
2458 Organization-Defined Parameter

2459 **OMB**
2460 Office of Management and Budget

2461 **OT**
2462 Operational Technology

2463 **PIN**
2464 Personal Identification Number

2465 **PLC**
2466 Programmable Logic Controller

2467 **PRA**
2468 Penetration-Resistant Architecture

2469 **ROI**
2470 Return on Investment

2471 **SCRM**
2472 Supply Chain Risk Management

2473 **SIEM**
2474 Security Information and Event Management

2475 **SOC**
2476 Security Operations Center

2477 **SP**
2478 Special Publication

2479 **TEE**
2480 Trusted Execution Environment

2481 **TPM**
2482 Trusted Platform Module

2483 **TTP**
2484 Tactics, Techniques, and Procedures

2485 **USC**
2486 United States Code

2487 **UEFI**
2488 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*.

2530 **confidentiality**
2531 Preserving authorized restrictions on information access and disclosure, including means for protecting personal
2532 privacy and proprietary information. [20]

2533 **configuration management**
2534 A collection of activities focused on establishing and maintaining the integrity of information technology products
2535 and systems through the control of processes for initializing, changing, and monitoring the configurations of those
2536 products and systems throughout the system development life cycle.

2537 **configuration settings**
2538 The set of parameters that can be changed in hardware, software, or firmware that affect the security posture or
2539 functionality of the system.

2540 **controlled unclassified information**
2541 Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating
2542 controls, excluding information that is classified under Executive Order 13526, Classified National Security
2543 Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as
2544 amended. [1]

2545 **critical program (or technology)**
2546 A program which significantly increases capability, mission effectiveness, or extends the expected effective life of
2547 an essential system/capability. [1]

2548 **CUI categories**
2549 Those types of information for which laws, regulations, or government-wide policies require or permit agencies to
2550 exercise safeguarding or dissemination controls and which the CUI Executive Agent has approved and listed in the
2551 CUI Registry. [5]

2552 **CUI Executive Agent**
2553 The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI
2554 Program and oversees federal agency actions to comply with Executive Order 13556. NARA has delegated this
2555 authority to the Director of the Information Security Oversight Office (ISOO). [5]

2556 **CUI program**
2557 The executive branch-wide program to standardize CUI handling by all federal agencies. The program includes the
2558 rules, organization, and procedures for CUI, established by Executive Order 13556, 32 CFR Part 2002, and the CUI
2559 Registry. [5]

2560 **cyber-physical system**
2561 Interacting digital, analog, physical, and human components engineered for function through integrated physics
2562 and logic.

2563 **cyber resiliency**
2564 The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or
2565 compromises on systems that use or are enabled by cyber resources. [13]

2566 **damage-limiting operations**
2567 Procedural and operational measures that use system capabilities to maximize the ability of an organization to
2568 detect successful system compromises by an adversary and to limit the effects of such compromises (both
2569 detected and undetected).

2570 **defense-in-depth**
2571 Information security strategy integrating people, technology, and operations capabilities to establish variable
2572 barriers across multiple layers and missions of the organization.

2573 **discussion**
2574 Statements used to provide additional explanatory information for security controls or security control
2575 enhancements.

2576 **disinformation**
2577 The process of providing deliberately deceptive information to adversaries to mislead or confuse them regarding
2578 the security posture of the system or organization or the state of cyber preparedness.

2579 **dual authorization**
2580 The system of storage and handling designed to prohibit individual access to certain resources by requiring the
2581 presence and actions of at least two authorized persons, each capable of detecting incorrect or unauthorized
2582 security procedures with respect to the task being performed. [16, adapted]

2583 **enhanced security requirements**
2584 Security requirements that can be implemented in addition to the requirements in NIST Special Publication 800-
2585 171. The additional security requirements provide the foundation for a defense-in-depth protection strategy that
2586 includes three mutually supportive and reinforcing components: (1) penetration-resistant architecture, (2)
2587 damage-limiting operations, and (3) cyber resiliency.

2588 **executive agency**
2589 An executive department specified in 5 U.S.C. Sec. 101; a military department specified in 5 U.S.C. Sec. 102; an
2590 independent establishment as defined in 5 U.S.C. Sec. 104(1); and a wholly owned Government corporation fully
2591 subject to the provisions of 31 U.S.C. Chapter 91. [18]

2592 **external network**
2593 A network not controlled by the organization.

2594 **external system (or component)**
2595 A system or component of a system that is outside of the authorization boundary established by the organization
2596 and for which the organization typically has no direct control over the application of required security controls or
2597 the assessment of security control effectiveness.

2598 **federal agency**
2599 See *executive agency*.

2600 **federal information system**
2601 An information system used or operated by an executive agency, by a contractor of an executive agency, or by
2602 another organization on behalf of an executive agency. [23]

2603 **firmware**
2604 Computer programs and data stored in hardware—typically in read-only memory (ROM) or programmable read-
2605 only memory (PROM)—such that programs and data cannot be dynamically written or modified during execution
2606 of the programs. See *hardware* and *software*.

2607 **hardware**
2608 The material physical components of a system. See *software* and *firmware*.

2609 **high value asset**
2610 A designation of federal information or a federal information system when it relates to one or more of the
2611 following categories:

2612 – *Informational Value*: The information or information system that processes, stores, or transmits the
2613   information is of high value to the Government or its adversaries.

2614 – *Mission-Essential*: The agency that owns the information or information system cannot accomplish its
2615   Primary Mission-Essential Functions (PMEF), as approved in accordance with Presidential Policy Directive

2616   40 (PPD-40) National Continuity Policy, within expected timelines without the information or information
2617   system.

2618   −   *Federal Civilian Enterprise Essential (FCEE)*: The information or information system serves a critical
2619   function in maintaining the security and resilience of the federal civilian enterprise. [10]

impact
2621 With respect to security, the effect on organizational operations, organizational assets, individuals, other
2622 organizations, or the Nation (including the national security interests of the United States) of a loss of
2623 confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that
2624 individuals could experience when an information system processes their PII.

impact value
2626 The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or
2627 availability of information expressed as a value of low, moderate, or high. [6]

incident
2629 An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or
2630 availability of information or an information system or constitutes a violation or imminent threat of violation of
2631 law, security policies, security procedures, or acceptable use policies. [20]

industrial Internet of Things
2633 The sensors, instruments, machines, and other devices that are networked together and use Internet connectivity
2634 to enhance industrial and manufacturing business processes and applications.

information
2636 Any communication or representation of knowledge, such as facts, data, or opinions in any medium or form,
2637 including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. [18]

information flow control
2639 Procedure to ensure that information transfers within a system are not made in violation of the security policy.

information resources
2641 Information and related resources, such as personnel, equipment, funds, and information technology. [24]

information security
2643 The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or
2644 destruction in order to provide confidentiality, integrity, and availability. [20]

information system
2646 A discrete set of information resources organized for the collection, processing, maintenance, use, sharing,
2647 dissemination, or disposition of information. [24]

information technology
2649 Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the
2650 automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display,
2651 switching, interchange, transmission, or reception of data or information by the agency. For purposes of this
2652 definition, such services or equipment if used by the agency directly or is used by a contractor under a contract
2653 with the agency that requires its use; or to a significant extent, its use in the performance of a service or the
2654 furnishing of a product. Information technology includes computers, ancillary equipment (including imaging
2655 peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment
2656 designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures,
2657 services (including cloud computing and help-desk services or other professional services which support any point
2658 of the life cycle of the equipment or service), and related resources. Information technology does not include any
2659 equipment that is acquired by a contractor incidental to a contract which does not require its use. [18]

2660 **insider threat**
2661 The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of
2662 the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized
2663 disclosure, or through the loss or degradation of departmental resources or capabilities.

2664 **integrity**
2665 Guarding against improper information modification or destruction and includes ensuring information non-
2666 repudiation and authenticity. [20]

2667 **Internet of Things**
2668 The network of devices that contain the hardware, software, firmware, and actuators which allow the devices to
2669 connect, interact, and freely exchange data and information.

2670 **malicious code**
2671 Software or firmware intended to perform an unauthorized process that will have an adverse impact on the
2672 confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that
2673 infects a host. Spyware and some forms of adware are also examples of malicious code.

2674 **media**
2675 Physical devices or writing surfaces, including but not limited to magnetic tapes, optical disks, magnetic disks,
2676 Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information
2677 is recorded, stored, or printed within a system. [7]

2678 **misdirection**
2679 The process of maintaining and employing deception resources or environments and directing adversary activities
2680 to those resources or environments.

2681 **mobile device**
2682 A portable computing device that has a small form factor such that it can easily be carried by a single individual; is
2683 designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses
2684 local, non-removable or removable data storage; and includes a self-contained power source. Mobile devices may
2685 also include voice communication capabilities, on-board sensors that allow the devices to capture information, or
2686 built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-
2687 readers.

2688 **moving target defense**
2689 The concept of controlling change across multiple system dimensions in order to increase uncertainty and
2690 apparent complexity for attackers, reduce their window of opportunity, and increase the costs of their probing and
2691 attack efforts.

2692 **mutual authentication**
2693 The process of both entities involved in a transaction verifying each other. See *bidirectional authentication*.

2694 **network**
2695 A system implemented with a collection of interconnected components. Such components may include routers,
2696 hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

2697 **network access**
2698 Access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local
2699 area network, wide area network, Internet).

2700 **nonfederal organization**
2701 An entity that owns, operates, or maintains a nonfederal system.

2702 **nonfederal system**
2703 A system that does not meet the criteria for a federal system.

2704   **on behalf of (an agency)**
2705   A situation that occurs when (i) a non-executive branch entity uses or operates an information system or maintains
2706   or collects information for the purpose of processing, storing, or transmitting federal information; and (ii) those
2707   activities are not incidental to providing a service or product to the Government. [5]

2708   **operational technology**
2709   The hardware, software, and firmware components of a system used to detect or cause changes in physical
2710   processes through the direct control and monitoring of physical devices.

2711   **organization**
2712   An entity of any size, complexity, or positioning within an organizational structure. [7, adapted]

2713   **penetration-resistant architecture**
2714   An architecture that uses technology and procedures to limit the opportunities for an adversary to compromise an
2715   organizational system and achieve a persistent presence in the system.

2716   **personnel security**
2717   The discipline of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties
2718   and responsibilities requiring trustworthiness. [8]

2719   **potential impact**
2720   The loss of confidentiality, integrity, or availability could be expected to have (i) a limited adverse effect (FIPS
2721   Publication 199 low); (ii) a serious adverse effect (FIPS Publication 199 moderate); or (iii) a severe or catastrophic
2722   adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals. [6]

2723   **privileged user**
2724   A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not
2725   authorized to perform.

2726   **records**
2727   The recordings (automated and manual) of evidence of activities performed or results achieved (e.g., forms,
2728   reports, test results), which serve as a basis for verifying that the organization and system are performing as
2729   intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a
2730   program and that contain the complete set of information on particular items).

2731   **remote access**
2732   Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an
2733   external network (e.g., the Internet).

2734   **replay resistant**
2735   Protection against the capture of transmitted authentication or access control information and its subsequent
2736   retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

2737   **risk**
2738   A measure of the extent to which an entity is threatened by a potential circumstance or event and typically is a
2739   function of (i) the adverse impact or magnitude of harm that would arise if the circumstance or event occurs and
2740   (ii) the likelihood of occurrence. [18]

2741   **risk assessment**
2742   The process of identifying risks to organizational operations (including mission, functions, image, reputation),
2743   organizational assets, individuals, other organizations, and the Nation resulting from the operation of a system.
2744   [21]

2745 **roots of trust**
2746 Highly reliable hardware, firmware, and software components that perform specific, critical security functions.
2747 Because roots of trust are inherently trusted, they must be secure by design. Roots of trust provide a firm
2748 foundation from which to build security and trust. [25]

2749 **sanitization**
2750 Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization,
2751 extraordinary means. Process to remove information from media such that data recovery is not possible.

2752 **security**
2753 A condition that results from the establishment and maintenance of protective measures that enable an
2754 organization to perform its mission or critical functions despite risks posed by threats to its use of systems.
2755 Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and
2756 correction that should form part of the organization's risk management approach.

2757 **security assessment**
2758 See *security control assessment*.

2759 **security control**
2760 The safeguards or countermeasures prescribed for an information system or an organization to protect the
2761 confidentiality, integrity, and availability of the system and its information. [18]

2762 **security control assessment**
2763 The testing or evaluation of security controls to determine the extent to which the controls are implemented
2764 correctly, operating as intended, and producing the desired outcome with respect to meeting the security
2765 requirements for an information system or organization. [18]

2766 **security domain**
2767 A domain that implements a security policy and is administered by a single authority. [16, adapted]

2768 **security functions**
2769 The hardware, software, or firmware of the system responsible for enforcing the system security policy and
2770 supporting the isolation of code and data on which the protection is based.

2771 **security solution**
2772 The key design, architectural, and implementation choices made by organizations in satisfying specified security
2773 requirements for systems or system components.

2774 **system**
2775 See *information system*.

2776 **system component**
2777 A discrete, identifiable information technology asset that represents a building block of a system and may include
2778 hardware, software, and firmware. [26]

2779 **system security plan**
2780 A document that describes how an organization meets the security requirements for a system or how an
2781 organization plans to meet the requirements. In particular, the system security plan describes the system
2782 boundary, the environment in which the system operates, how security requirements are implemented, and the
2783 relationships with or connections to other systems.

2784 **system service**
2785 A capability provided by a system that facilitates information processing, storage, or transmission.

2786   **tactics, techniques, and procedures**
2787   The behavior of an actor. A tactic is the highest-level description of the behavior; techniques provide a more
2788   detailed description of the behavior in the context of a tactic; and procedures provide a lower-level, highly detailed
2789   description of the behavior in the context of a technique. [14]

2790   **tainting**
2791   The process of embedding covert capabilities in information, systems, or system components to allow
2792   organizations to be alerted to the exfiltration of information.

2793   **threat**
2794   Any circumstance or event with the potential to adversely impact organizational operations, organizational assets,
2795   individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure,
2796   modification of information, and/or denial of service. [21]

2797   **threat information**
2798   Any information related to a threat that might help an organization protect itself against the threat or detect the
2799   activities of an actor. Major types of threat information include indicators, TTPs, security alerts, threat intelligence
2800   reports, and tool configurations. [14]

2801   **threat intelligence**
2802   Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the
2803   necessary context for decision-making processes. [14]

2804   **Appendix C. Summary of Enhanced Security Requirements**

2805   This appendix provides a consolidated list of the enhanced security requirements in Sec. 3.

2806   **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

2808   **Appendix D. Adversary Effects**

2809   Cyber resiliency solutions are only relevant if they have some effect on risk, specifically by
2810   reducing the likelihood of the occurrence of threat events,[20] the ability of threat events to
2811   cause harm, and the extent of that harm.[21] The types of analysis of system architectures,
2812   designs, implementations, and operations that are indicated for cyber resiliency can include
2813   considering the effects that alternatives could have on the threat events in scenarios of concern
2814   to organizations.

2815   From the perspective of protecting a system against adversarial threats, five high-level, desired
2816   effects on the adversary can be identified: *redirect*, *preclude*, *impede*, *limit*, and *expose*. These
2817   effects are useful for discussion but are often too general to facilitate the definition of specific
2818   measures of effectiveness. Therefore, more specific classes of effects are defined:

2819   - *Deter*, *divert*, and *deceive* in support of **redirect**

2820   - *Negate*, *preempt*, and *expunge* in support of **preclude**

2821   - *Contain*, *degrade*, *delay*, and *exert* in support of **impede**

2822   - *Shorten* and *reduce* in support of **limit**

2823   - *Detect*, *reveal*, and *scrutinize* in support of **expose**

2824   These effects are tactical (i.e., local to a specific threat event or scenario), although it is possible
2825   that their repeated achievement could have strategic effects as well.

2826   Table 3 defines the effects, indicates how each effect could reduce risk, and illustrates how the
2827   use of certain approaches to implementing cyber resiliency techniques for protection against
2828   attack could have the identified effect.[22] The term "defender" refers to the organization or
2829   organizational staff responsible for providing or applying protections. It should be noted that
2830   likelihoods and impact can be reduced, but risk cannot be eliminated. Thus, no effect can be
2831   assumed to be complete, even those with names that suggest completeness, such as negate,
2832   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

2835   **Appendix E. Organization-Defined Parameters**

2836   This appendix lists the organization-defined parameters (ODPs) that are included in the
2837   enhanced security requirements in Sec. 3. The ODPs are listed sequentially by requirement
2838   family, beginning with the first requirement containing an ODP in the Access Control (AC) family
2839   and ending with the last requirement containing an ODP in the Supply Chain Risk Management
2840   (SR) family. Embedded ODPs are listed as a single entry in the table.

2841   **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*]]

2842 **Appendix F. Change Log**

2843 This publication incorporates the following changes from the original edition (February 2,
2844 2021):

2845 • Streamlined introductory information in Sec. 1 and Sec. 2 to improve clarity and
2846   understanding

2847 • Increased the specificity of the enhanced security requirements to remove ambiguity,
2848   improve the effectiveness of implementation, and clarify the scope of assessments

2849 • Grouped enhanced security requirements, where possible, to improve understanding
2850   and the efficiency of implementations and assessments

2851 • Removed outdated and redundant enhanced security requirements

2852 • Added new enhanced security requirements based on (1) the latest threat intelligence,
2853   (2) empirical data from cyber-attacks, and (3) the expansion of security objectives to
2854   include integrity and availability

2855 • Added titles to the enhanced security requirements

2856 • Restructured and streamlined the security requirement discussion sections

2857 • Revised the enhanced security requirements for consistency with the security control
2858   language in SP 800-53

2859 • Revised the structure of the References, Acronyms, and Glossary sections for greater
2860   clarity and ease of use

2861 • Added Appendix C to summarize the enhanced security requirements

2862 • Added Appendix E to list organization-defined parameters for the enhanced security
2863   requirements

2864 • Removed an appendix with a mapping table for security controls and protection
2865   strategies and transferred that information to the individual security requirements in
2866   Sec. 3

2867 • Implemented a one-time "revision number" change for consistency with SP 800-171r3

2868 Table 5 shows the changes incorporated into this publication. Errata updates can include
2869 corrections, clarifications, or other minor changes in the publication that are either *editorial* or
2870 *substantive* in nature. Any potential updates to this document that are not yet published in an
2871 errata update or a formal revision, including additional issues and potential corrections, will be
2872 posted as they are identified. See the [publication details](#) for this report. The current release of
2873 this publication does not include any errata updates.

2874   **Table 5. Change Log**

PUBLICATION ID	DATE	TYPE OF EDIT	CHANGE	LOCATION

2875