Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes.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

Withdrawal Date May 14, 2024

Original Release Date November 9, 2023

The attached draft document is followed by:

Status Final

Series/Number NIST SP 800-171Ar3

Title Assessing Security Requirements for Controlled Unclassified

Information

Publication Date May 2024

DOI https://doi.org/10.6028/NIST.SP.800-171Ar3

CSRC URL https://csrc.nist.gov/pubs/sp/800/171/a/r3/final

Additional Information





NIST Special Publication NIST SP 800-171Ar3 ipd

Assessing Security Requirements for Controlled Unclassified Information

Initial Public Draft

Ron Ross Victoria Pillitteri

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-171Ar3.ipd



NIST Special Publication NIST SP 800-171Ar3 ipd

Assessing Security Requirements for Controlled Unclassified Information

Initial Public Draft

Ron Ross Victoria Pillitteri Computer Security Division Information Technology Laboratory

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-171Ar3.ipd

November 2023



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

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

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

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

NIST Technical Series Policies

<u>Copyright, Use, and Licensing Statements</u> NIST Technical Series Publication Identifier Syntax

How to Cite this NIST Technical Series Publication:

Ross R, Pillitteri V (2023) Assessing Security Requirements for Controlled Unclassified Information and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171Ar3 ipd. https://doi.org/10.6028/NIST.SP.800-171Ar3.ipd

Author ORCID iDs

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

Public Comment Period

November 9, 2023 – January 26, 2024 (originally Jan. 12, 2024)

Submit Comments

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

All comments 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 and nonfederal organizations with assessment procedures and a
- 6 methodology that can be employed to conduct assessments of the security requirements in NIST
- 7 Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal
- 8 Systems and Organizations. The assessment procedures are flexible and can be customized to the
- 9 needs of organizations and assessors. Security assessments can be conducted as independent,
- third-party assessments or as government-sponsored assessments. The assessments can also be
- applied with various degrees of rigor based on customer-defined depth and coverage attributes.
- 12 The findings and evidence produced during the assessments can facilitate risk-based decisions by
- organizations related to the security requirements.

14 Keywords

- assessment; assessment method; assessment object; assessment procedure; assurance; basic
- security requirement; controlled unclassified information; coverage; CUI registry; depth;
- 17 Executive Order 13556; FISMA; NIST Special Publication 800-171; NIST Special Publication
- 18 800-53A; nonfederal organization; nonfederal system; security assessment; security control.

19 Reports on Computer Systems Technology

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

30 Audience

40

41

43

- This publication serves a diverse group of individuals and organizations in the public and private sectors, including individuals with:
- System development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, system/security engineers, systems integrators)
- Acquisition or procurement responsibilities (e.g., contracting officers)
- System, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers)
 - Security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts)
- The above roles and responsibilities can be viewed from two perspectives:
 - Federal perspective: The entity establishing and conveying security assessment requirements in contractual vehicles or other types of agreements
- *Nonfederal perspective*: The entity responding to and complying with security assessment requirements set forth in contracts or agreements

47 Note to Reviewers

- 48 This update to NIST Special Publication (SP) 800-171A represents over one year of data
- 49 collection, technical analysis, customer interaction, redesign, and development of the procedures
- 50 for assessing the security requirements for Controlled Unclassified Information (CUI). Many
- 51 trade-offs have been made to ensure that the assessment procedures have been stated clearly and
- 52 concisely while also recognizing the specific needs of both federal and nonfederal organizations.
- The following significant changes have been made in the initial public draft (ipd) of NIST SP
- 54 800-171A, Revision 3:
- The restructuring of the assessment procedure syntax to align with NIST SP 800-53A [5].
- The addition of a references section to provide source assessment procedures from NIST SP 800-53A [5].
- There has also been a one-time change to the publication version number to align with NIST SP
- 59 800-171, Revision 3 [3].
- NIST is specifically interested in comments, feedback, and recommendations for the following
- 61 topics:
- The alignment of the assessment procedures to NIST SP 800-53A [5].
- The use of organization-defined parameters (ODPs) in the assessment procedures.
- The ease-of-use of the assessment procedures in conducting assessments of the CUI security requirements.
- 66 Reviewers are encouraged to comment on all or parts of NIST SP 800-171A, Revision 3 ipd.
- NIST requests that all comments be submitted to 800-171comments@list.nist.gov by 11:59 p.m.
- Eastern Standard Time (EST) on **January 12, 2024**. Commenters are encouraged to use the
- 69 comment template provided with the document announcement.
- 70 Comments received in response to this request will be posted on the Protecting CUI project site
- 71 after the due date. Submitters' names and affiliations (when provided) will be included, while
- 72 contact information will be removed.

Call for Patent Claims

73

82

83

84

85

8687

88 89

- 74 This public review includes a call for information on essential patent claims (claims whose use
- 75 would be required for compliance with the guidance or requirements in this Information
- 76 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be
- directly stated in this ITL Publication or by reference to another publication. This call also
- 78 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications
- 79 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.
- 80 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, 81 in written or electronic form, either:
 - a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or
 - b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:
 - i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
 - ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.
- 91 Such assurance shall indicate that the patent holder (or third party authorized to make assurances
- on its behalf) will include in any documents transferring ownership of patents subject to the
- assurance, provisions sufficient to ensure that the commitments in the assurance are binding on
- 94 the transferee, and that the transferee will similarly include appropriate provisions in the event of
- 95 future transfers with the goal of binding each successor-in-interest.
- The assurance shall also indicate that it is intended to be binding on successors-in-interest
- 97 regardless of whether such provisions are included in the relevant transfer documents.
- 98 Such statements should be addressed to: 800-171comments@list.nist.gov

Table of Contents

100	1. Introduction	1
101	1.1. Purpose and Applicability	1
102	1.2. Organization of This Publication	1
103	2. The Fundamentals	3
104	2.1. Assessment Procedures	3
105	2.2. Assurance Cases	5
106	3. The Procedures	7
107	3.1. Access Control	7
108	3.1.1. Account Management	7
109	3.1.2. Access Enforcement	8
110	3.1.3. Information Flow Enforcement	9
111	3.1.4. Separation of Duties	9
112	3.1.5. Least Privilege	10
113	3.1.6. Least Privilege – Privileged Accounts	11
114	3.1.7. Least Privilege – Privileged Functions	11
115	3.1.8. Unsuccessful Logon Attempts	12
116	3.1.9. System Use Notification	
117	3.1.10. Device Lock	13
118	3.1.11. Session Termination	14
119	3.1.12. Remote Access	14
120	3.1.13. Withdrawn	15
121	3.1.14. Withdrawn	15
122	3.1.15. Withdrawn	15
123	3.1.16. Wireless Access	16
124	3.1.17. Withdrawn	16
125	3.1.18. Access Control for Mobile Devices	16
126	3.1.19. Withdrawn	17
127	3.1.20. Use of External Systems	17
128	3.1.21. Withdrawn	18
129	3.1.22. Publicly Accessible Content	18
130	3.2. Awareness and Training	
131	3.2.1. Literacy Training and Awareness	19
132	3.2.2. Role-Based Training	
133	3.2.3. Withdrawn	
134	3.3. Audit and Accountability	21

NIST SP 800-171Ar3 ipd (Initial Public Draft) November 2023

135	3.3.1.	Event Logging	21
136	3.3.2.	Audit Record Content	21
137	3.3.3.	Audit Record Generation	22
138	3.3.4.	Response to Audit Logging Process Failures	23
139	3.3.5.	Audit Record Review, Analysis, and Reporting	23
140	3.3.6.	Audit Record Reduction and Report Generation	24
141	3.3.7.	Time Stamps	25
142	3.3.8.	Protection of Audit Information	25
143	3.3.9.	Withdrawn	26
144	3.4. Co	nfiguration Management	26
145	3.4.1.	Baseline Configuration	26
146	3.4.2.	Configuration Settings	27
147	3.4.3.	Configuration Change Control	28
148	3.4.4.	Impact Analyses	28
149	3.4.5.	Access Restrictions for Change	29
150	3.4.6.	Least Functionality	30
151	3.4.7.	Withdrawn	31
152	3.4.8.	Authorized Software – Allow by Exception	31
153	3.4.9.	Withdrawn	32
154	3.4.10	System Component Inventory	32
155	3.4.11	. Information Location	33
156	3.4.12	. System and Component Configuration for High-Risk Areas	34
157	3.5. Ide	entification and Authentication	34
158	3.5.1.	User Identification, Authentication, and Re-Authentication	34
159	3.5.2.	Device Identification and Authentication	35
160	3.5.3.	Multi-Factor Authentication	36
161	3.5.4.	Replay-Resistant Authentication	36
162	3.5.5.	Identifier Management	37
163	3.5.6.	Withdrawn	37
164	3.5.7.	Password Management	37
165	3.5.8.	Withdrawn	38
166	3.5.9.	Withdrawn	38
167	3.5.10	. Withdrawn	38
168	3.5.11	. Authentication Feedback	39
169	3.5.12	. Authenticator Management	39
170	3.6. Inc	ident Response	40

171	3.6.1.	Incident Response Plan and Handling	40
172	3.6.2.	Incident Monitoring, Reporting, and Response Assistance	41
173	3.6.3.	Incident Response Testing	42
174	3.6.4.	Incident Response Training	42
175	3.7. Ma	aintenance	43
176	3.7.1.	Withdrawn	43
177	3.7.2.	Withdrawn	43
178	3.7.3.	Withdrawn	43
179	3.7.4.	Maintenance Tools	43
180	3.7.5.	Nonlocal Maintenance	44
181	3.7.6.	Maintenance Personnel	45
182	3.8. Me	edia Protection	46
183	3.8.1.	Media Storage	46
184	3.8.2.	Media Access	46
185	3.8.3.	Media Sanitization	47
186	3.8.4.	Media Marking	47
187	3.8.5.	Media Transport	48
188	3.8.6.	Withdrawn	49
189	3.8.7.	Media Use	49
190	3.8.8.	Withdrawn	49
191	3.8.9.	System Backup – Cryptographic Protection	50
192	3.9. Pe	rsonnel Security	50
193	3.9.1.	Personnel Screening	50
194	3.9.2.	Personnel Termination and Transfer	51
195	3.10. Ph	ysical Protection	52
196	3.10.1	. Physical Access Authorizations	52
197	3.10.2	. Monitoring Physical Access	53
198	3.10.3	. Withdrawn	53
199	3.10.4	. Withdrawn	53
200	3.10.5	. Withdrawn	53
201	3.10.6	. Alternate Work Site	53
202	3.10.7	. Physical Access Control	54
203	3.10.8	. Access Control for Transmission and Output Devices	55
204	3.11. Ris	sk Assessment	56
205	3.11.1	. Risk Assessment	56
206	3.11.2	. Vulnerability Monitoring and Scanning	56

207	3.11.3. Withdrawn	57
208	3.12. Security Assessment and Monitoring	57
209	3.12.1. Security Assessment	57
210	3.12.2. Plan of Action and Milestones	58
211	3.12.3. Continuous Monitoring	59
212	3.12.4. Withdrawn	59
213	3.12.5. Information Exchange	59
214	3.13. System and Communications Protection	60
215	3.13.1. Boundary Protection	60
216	3.13.2. Withdrawn	61
217	3.13.3. Withdrawn	61
218	3.13.4. Information in Shared System Resources	
219	3.13.5. Withdrawn	62
220	3.13.6. Network Communications – Deny by Default – Allow by Exception	62
221	3.13.7. Withdrawn	
222	3.13.8. Transmission and Storage Confidentiality	
223	3.13.9. Network Disconnect	
224	3.13.10. Cryptographic Key Establishment and Management	
225	3.13.11. Cryptographic Protection	
226	3.13.12. Collaborative Computing Devices and Applications	
227	3.13.13. Mobile Code	
228	3.13.14. Withdrawn	
229	3.13.15. Session Authenticity	
230	3.13.16. Withdrawn	
231	3.14. System and Information Integrity	
232	3.14.1. Flaw Remediation	
233	3.14.2. Malicious Code Protection	
234	3.14.3. Security Alerts, Advisories, and Directives	
235	3.14.4. Withdrawn	
236	3.14.5. Withdrawn	
237	3.14.6. System Monitoring	
238	3.14.7. Withdrawn	
239	3.14.8. Information Management and Retention	
240	3.15. Planning	
241	3.15.1. Policy and Procedures	
242	3.15.2. System Security Plan	/2

243	3.15.3. Ri	ules of Behavior	73
244	3.16. Syste	m and Services Acquisition	74
245	3.16.1. Ad	equisition Process	74
246	3.16.2. Uı	nsupported System Components	74
247	3.16.3. Ex	kternal System Services	75
248	3.17. Suppl	y Chain Risk Management	76
249	3.17.1. St	upply Chain Risk Management Plan	76
250	3.17.2. Ad	equisition Strategies, Tools, and Methods	77
251	3.17.3. St	upply Chain Requirements and Processes	78
252	References		79
253	Appendix A.	Acronyms	80
254	Appendix B.	Glossary	81
255	Appendix C.	Change Log	83
256			

NIST SP 800-171Ar3	ipd (Initial Public Draft)
November 2023	

Assessing CUI Security Requirements

257	List of Tables	
258	Table 1. Security requirement families	3
259	Table 2. Change Log	
260		

261 Acknowledgments

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

268 Historical Contributions

- 269 The authors wish to acknowledge the following individuals for their historic contributions to this
- 270 publication: Jon Boyens, Devin Casey, Chris Enloe, Ned Goren, Gary Guissanie, Jody Jacobs,
- 271 Jeff Marron, Vicki Michetti, Mark Riddle, Mary Thomas, Gary Stoneburner, Patricia Toth, and
- 272 Patrick Viscuso.

273 1. Introduction

284

294

296

297

298

299

300

301

- The security assessment process gathers information and produces evidence to determine the effectiveness of security requirements by:
- Identifying potential problems or shortfalls in security and risk management programs;
- Identifying security weaknesses and deficiencies in systems and the environments in which those systems operate;
- Prioritizing risk mitigation decisions and activities;
- Confirming that identified security weaknesses and deficiencies in the system and environment of operation have been addressed; and
- Supporting continuous monitoring activities and providing information security situational awareness.

1.1. Purpose and Applicability

- 285 The purpose of this publication is to provide procedures for assessing the security requirements
- in NIST Special Publication (SP) 800-171, Protecting Controlled Unclassified Information
- 287 (CUI) in Nonfederal Systems and Organizations [3]. Organizations can use the assessment
- procedures to generate evidence to support the assertion that the security requirements have been
- satisfied. The scope of the security assessments conducted using the procedures described in this
- publication are guided and informed by the system security plans for systems that process, store,
- or transmit CUI. The assessment procedures offer the flexibility to customize assessments based
- on organizational policies and requirements, known threat and vulnerability information, system
- and platform dependencies, operational considerations, and tolerance for risk.¹

1.2. Organization of This Publication

- 295 The remainder of this special publication is organized as follows:
 - <u>Section 2</u> describes the fundamental concepts associated with assessments of security requirements, including assessment procedures, methods, objects, and assurance cases that can be created using evidence produced during assessments.
 - <u>Section 3</u> provides assessment procedures for the security requirements in NIST SP 800-171, including assessment objectives and potential assessment methods and objects for each procedure.
- The following sections provide additional information to support the protection of CUI in nonfederal systems and organizations:
- References
- Appendix A: Acronyms

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

- Appendix B: Glossary
- Appendix C: Change Log

308

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

2. The Fundamentals

- 311 The process used by organizations and assessors to assess the security requirements in NIST SP
- 312 800-171 includes (1) preparing for the assessment, (2) developing a security assessment plan, (3)
- 313 conducting the assessment, and (4) documenting, analyzing, and reporting the assessment
- 314 results.² The remainder of this section describes the structure and content of the procedures used
- 315 to assess the security requirements and the importance of assurance cases in providing the
- evidence necessary to determine compliance with the requirements.

2.1. Assessment Procedures

- The security requirements in NIST SP 800-171 are organized into 17 families, as illustrated in
- Table 1. The assessment procedures in <u>Section 3</u> are grouped by similar family designations to
- ensure the completeness and consistency of assessments. The procedures have been derived from
- the assessment procedures in NIST SP 800-53A [5].

Table 1. Security requirement families

Access Control	<u>Maintenance</u>	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
<u>Identification and Authentication</u>	Risk Assessment	System and Services Acquisition
<u>Incident Response</u>		Supply Chain Risk Management

323

310

- 324 An assessment procedure consists of an assessment *objective* and a set of potential assessment
- 325 methods and objects that can be used to conduct the assessment. Each potential assessment
- 326 objective includes a determination statement related to the security requirement. If there is an
- 327 organization-defined parameter (ODP) in the security requirement, then the assessment objective
- begins with a determination statement related to the definition of the ODP. The determination
- statements are linked to the content of the security requirements to help ensure traceability of the
- assessment results to the requirements.
- Assessment objects identify the specific items being assessed and can include specifications,
- mechanisms, activities, and individuals. Specifications are the documented artifacts³ (e.g., plans,
- policies, procedures, requirements, functional and assurance specifications, architectures, and
- design documentation) associated with a system. Mechanisms are the hardware, software, and
- firmware safeguards implemented within a system. Activities are the protection-related actions
- supporting a system that involve people (e.g., conducting system backup operations, exercising
- an incident response plan, and monitoring network traffic). Individuals are the people applying
- the specifications, mechanisms, or activities described above.

² NIST SP 800-53A [5] provides additional information on the assessment process and the individuals steps listed above.

³ Artifacts may be in formats other than documents (e.g., databases, Governance, Risk, and Compliance [GRC] tools, or Open Security Controls Assessment Language [OSCAL])

- 339 Assessment methods define the nature and extent of the assessor's actions and are used to 340 facilitate understanding, achieve clarification, or obtain evidence. The potential assessment 341 methods include examine, interview, and test. The examine method is the process of reviewing, 342 studying, inspecting, observing, or analyzing assessment objects. The interview method is the process of holding discussions with individuals or groups about assessment objects. The test 343 344 method is the process of exercising assessment objects (i.e., activities, mechanisms) under 345 specified conditions to compare actual with expected behavior. Assessment methods include 346 attributes of depth and coverage, which define the rigor, scope, and level of effort for the
- 347 assessment as well as the degree of assurance that the security requirements have been satisfied.
- 348 The structure and content of a typical assessment procedure are provided in the example below:

372 373

374

375

376

377

378

379

349	3.1.8 Unsuccessful Logon Attempts	Security Requirement Na	ime	
350	REQUIREMENT: 03.01.08			
351	ASSESSMENT OBJECTIVE			
352	Determine if:	[
353 354	A.03.01.08.ODP[01]: the number of conse attempts by a user allowed during a time			Part Determination Statement curity Requirement and ODPs
355 356	A.03.01.08.ODP[02]: the time period to we consecutive invalid logon attempts by a		<i>I</i> .	
357 358	A.03.01.08: the number of consecutive inva <03.01.08.ODP[02]: time period> is limited			
359	ASSESSMENT METHODS AND OBJECTS	3		
360	Examine			
361 362 363	[SELECT FROM: access control policy and system design documentation; system audit other relevant documents or records]			
364	Interview			
365 366	[SELECT FROM: personnel with information administrators]	n security responsibilities;	system o	developers; system
367	Test			
368	[SELECT FROM: mechanisms implementing	g access control policy for	unsucce	essful logon attempts]
369	REFERENCES			
370	Source Assessment Procedure: AC-07			
371	Determination statements have alphanume	eric identifiers. Each d	letermi	nation statement begins

with the letter "A" to indicate that it is part of an assessment procedure. The next sequence of numbers and/or letters (e.g., 03.01.01.e or 03.01.01.f.02) indicates the security requirement identifier from SP 800-171 (and the specific control item if it is a multi-part requirement) that is the target of the assessment. Organization-defined parameters are indicated by the letters "**ODP**." If there are multiple ODPs in the determination statement, the ODP number is indicated in a square bracket (e.g., A.03.01.08.ODP[01]). Square brackets are also used to denote when an assessment procedure further decomposes a requirement into more granular determination statements (e.g., A.03.01.12.a[01], A.03.01.12.a[02], A.03.01.12.a[03]).

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

393

- For assessment findings that are other than satisfied, organizations may define subcategories of
- findings to indicate the severity or criticality of the weaknesses or deficiencies discovered and
- 390 the potential adverse effects of those weaknesses or deficiencies on the missions and/or business
- 391 functions of the organization. Defining such subcategories can help to establish priorities for
- 392 needed risk mitigation actions.

2.2. Assurance Cases

- 394 Building an effective assurance case to determine compliance with security requirements is a
- 395 process that involves compiling evidence from a variety of sources and conducting different
- 396 types of activities during an assessment. An assurance case is a body of evidence organized into
- an argument demonstrating that some claim about a system is true. For assessments conducted
- using the procedures in this publication, that claim is compliance with the security requirements
- in NIST SP 800-171. Assessors obtain evidence during security assessments to allow designated
- officials⁴ to make objective determinations about compliance with the security requirements. The
- 401 evidence needed to make such determinations can be obtained from various sources, including
- independent, third-party assessments or other types of assessments, depending on the needs of
- 403 the organization establishing the requirements and the organization conducting the assessments.
- 404 For example, many technical security requirements are satisfied by security capabilities that are
- built into commercial information technology products and systems. Product assessments are
- 406 typically conducted by independent, third-party testing organizations. ⁵ These assessments
- 407 examine the security functions of products and established configuration settings. Assessments
- 408 can also be conducted to demonstrate compliance with industry, national, or international
- security standards as well as developer and vendor claims. Since many information technology
- 410 products are assessed by commercial testing organizations and then subsequently deployed in
- 411 hundreds of thousands of systems, these types of assessments can be carried out at a greater level
- of depth and provide deeper insights into the security capabilities of the products.
- The evidence needed to determine compliance comes from assessing the implementation of the
- 414 safeguards and countermeasure selected to satisfy the security requirements. Assessors can build
- on previously developed materials that started with the specification of the information security

⁴ A designated official is an official, either internal or external to a nonfederal organization, with the responsibility to determine organizational compliance with the security requirements.

⁵ Examples of third-party testing organizations include Common Criteria Testing Laboratories that evaluate IT products in accordance with ISO/IEC 15408 [6] and Cryptographic Module Validation Program Testing Laboratories that evaluate cryptographic modules in accordance with Federal Information Processing Standard (FIPS) 140 [7].

416	needs of the organization and were further improved during the design, development, and
417	implementation of the system. These materials provide the initial evidence for an assurance case.
418	Assessments can be conducted by system developers, system integrators, auditors, system
419	owners, or the security staffs of organizations. The assessors or assessment teams bring together
420	available information about the system, such as the results of component product assessments.
421	The assessors can conduct additional system-level assessments using the assessment methods
422	and procedures contained in this publication and based on the implementation information
423	provided by the nonfederal organization in its system security plan. Assessments can be used to
424	compile and evaluate the evidence needed by organizations to help determine the effectiveness
425	of the safeguards implemented to protect CUI, the actions needed to mitigate security risks to the
426	organization, and compliance with the security requirements.

427 **3. The Procedures**

- This section provides assessment procedures for the security requirements defined in NIST SP
- 429 800-171. Organizations that conduct security requirement assessments can develop their security
- assessment plans by using the information provided in the assessment procedures and selecting
- 431 the specific assessment methods and objects that meet the organization's needs. Organizations
- also have flexibility in defining the level of rigor and detail associated with the assessment based
- on the assurance requirements of the organization.

3.1. Access Control

3.1.1. Account Management

- 436 **REQUIREMENT:** 03.01.01
- 437 ASSESSMENT OBJECTIVE
- 438 Determine if:

434

- 439 A.03.01.01.ODP[01]: time period for account inactivity before disabling is defined.
- **A.03.01.01.a[01]:** system account types allowed are defined.
- **A.03.01.01.a[02]:** system account types prohibited are defined.
- **A.03.01.01.b[01]:** system accounts are created in accordance with organizational policy,
- procedures, prerequisites, and criteria.
- **A.03.01.01.b[02]:** system accounts are enabled in accordance with organizational policy,
- procedures, prerequisites, and criteria.
- **A.03.01.01.b[03]:** system accounts are modified in accordance with organizational policy,
- procedures, prerequisites, and criteria.
- 448 **A.03.01.01.b[04]:** system accounts are disabled in accordance with organizational policy,
- procedures, prerequisites, and criteria.
- 450 **A.03.01.01.b[05]:** system accounts are removed in accordance with organizational policy,
- procedures, prerequisites, and criteria.
- **A.03.01.01.c[01]:** authorized users of the system are specified.
- **A.03.01.01.c[02]:** group and role membership are specified.
- **A.03.01.01.c[03]:** access authorizations (i.e., privileges) are specified.
- **A.03.01.01.d[01]:** access to the system is authorized based on a valid access authorization.
- **A.03.01.01.d[02]**: access to the system is authorized based on intended system usage.
- **A.03.01.01.e:** the use of system accounts is monitored.
- 458 **A.03.01.01.f.01:** system accounts are disabled when the accounts have expired.
- **A.03.01.01.f.02:** system accounts are disabled when the accounts have been inactive for
- 460 **<A.03.01.01.ODP[01]** time period>.
- **A.03.01.01.f.03:** system accounts are disabled when the accounts are no longer associated with
- 462 a user or individual.
- **A.03.01.01.f.04:** system accounts are disabled when the accounts violate organizational policy.

464 465		A.03.01.01.f.05: system accounts are disabled when significant risks associated with individuals are discovered.
466 467		A.03.01.01.g.01: organizational personnel or roles are notified when accounts are no longer required.
468 469		A.03.01.01.g.02: organizational personnel or roles are notified when users are terminated or transferred.
470 471		A.03.01.01.g.03: organizational personnel or roles are notified when system usage or the need-to-know changes for an individual.
472		ASSESSMENT METHODS AND OBJECTS
473		Examine
474 475 476 477 478 479 480 481 482 483		[SELECT FROM: access control policy and procedures; personnel termination/transfer policies and procedures; procedures for account management; system design documentation; system configuration settings; list of active system accounts and the name of the individual associated with each account; notifications of recent transfers, separations, or terminations of employees; list of conditions for group and role membership; list of recently disabled system accounts and the name of the individual associated with each account; list of user activities that pose significant organizational risks; access authorization records; account management compliance reviews; system monitoring and audit records; system security plan; system-generated list of accounts removed; system-generated list of emergency accounts disabled; system-generated list of disabled accounts; other relevant documents and records]
484		Interview
485 486		[SELECT FROM: personnel with account management responsibilities; system administrators; personnel with information security responsibilities; system developers]
487		Test
488 489		[SELECT FROM: processes for account management on the system; mechanisms for implementing account management]
490		REFERENCES
491		Source Assessment Procedures: <u>AC-02</u> , <u>AC-02(03)</u> , <u>AC-02(13)</u>
492	3.1.2.	Access Enforcement
493		REQUIREMENT: 03.01.02
494		ASSESSMENT OBJECTIVE
495		Determine if:
496 497		A.03.01.02: approved authorizations for logical access to CUI and system resources are enforced.
498		ASSESSMENT METHODS AND OBJECTS
499		Examine
500 501 502		[SELECT FROM: access control policy and procedures; procedures for access enforcement; system design documentation; system configuration settings; list of approved authorizations (i.e., user privileges); system audit records; system security plan; other relevant documents or records

503		Interview
504 505		[SELECT FROM: personnel with access enforcement responsibilities; system administrators; personnel with information security responsibilities; system developers]
506		Test
507		[SELECT FROM: mechanisms for implementing the access control policy]
508		REFERENCES
509		Source Assessment Procedure: <u>AC-03</u>
510	3.1.3.	Information Flow Enforcement
511		REQUIREMENT: 03.01.03
512		ASSESSMENT OBJECTIVE
513		Determine if:
514 515		A.03.01.03: approved authorizations are enforced for controlling the flow of CUI within the system and between connected systems.
516		ASSESSMENT METHODS AND OBJECTS
517		Examine
518 519 520 521		[SELECT FROM: access control policy and procedures; information flow control policies; procedures for information flow enforcement; security architecture and design documentation; system configuration settings; system baseline configuration; system audit records; list of information flow authorizations; system security plan; other relevant documents or records]
522		Interview
523 524		[SELECT FROM: system administrators; personnel with security architecture responsibilities; personnel with information security responsibilities; system developers]
525		Test
526		[SELECT FROM: mechanisms for implementing the information flow enforcement policy]
527		REFERENCES
528		Source Assessment Procedure: <u>AC-04</u>
529	3.1.4.	Separation of Duties
530		REQUIREMENT: 03.01.04
531		ASSESSMENT OBJECTIVE
532		Determine if:
533		A.03.01.04.a: duties of individuals requiring separation are identified.
534		A.03.01.04.b: system access authorizations to support separation of duties are defined.

535 ASSESSMENT METHODS AND OBJECTS 536 **Examine** 537 [SELECT FROM: access control policy and procedures; procedures for the separation of duties 538 and the division of responsibilities; system configuration settings; system audit records; system 539 access authorizations; list of divisions of responsibility and separation of duties; system security 540 plan; other relevant documents or records] 541 Interview 542 [SELECT FROM: personnel with responsibilities for defining the separation of duties and the 543 division of responsibilities; personnel with information security responsibilities; system 544 administrators1 545 **Test** 546 [SELECT FROM: mechanisms for implementing the separation of duties policy] 547 REFERENCES0 548 Source Assessment Procedure: AC-05 549 3.1.5. Least Privilege 550 REQUIREMENT: 03.01.05 551 **ASSESSMENT OBJECTIVE** 552 Determine if: 553 A.03.01.05.ODP[01]: security functions for authorized access are defined. 554 A.03.01.05.ODP[02]: security-relevant information for authorized access is defined. 555 A.03.01.05.a: system access for users (or processes acting on behalf of users) is authorized only 556 when necessary to accomplish assigned organizational tasks. 557 **A.03.01.05.b[01]**: access to **<A.03.01.05.ODP[01]** security functions**>** is authorized. 558 A.03.01.05.b[02]: access to <A.03.01.05.ODP[01] security-relevant information> is 559 authorized. 560 A.03.01.05.c: the privileges assigned to roles or classes of users are periodically reviewed to 561 validate the need for such privileges. 562 A.03.01.05.d: privileges are reassigned or removed, as necessary. 563 **ASSESSMENT METHODS AND OBJECTS** 564 **Examine** 565 [SELECT FROM: access control policy and procedures; procedures for least privilege; list of 566 assigned access authorizations (i.e., privileges); system configuration settings; system audit 567 records: list of security functions (deployed in hardware, software, and firmware); security-568 relevant information for which access must be explicitly authorized; list of system-generated roles 569 or classes of users and assigned privileges; validation reviews of privileges assigned to roles or 570 classes or users; records of privilege removals or reassignments for roles or classes of users; 571 system design documentation; system security plan; other relevant documents or records]

572		Interview
573 574		[SELECT FROM: personnel with responsibilities for defining least privileges; personnel with information security responsibilities; system administrators]
575		Test
576 577		[SELECT FROM: mechanisms for implementing least privilege functions; mechanisms for implementing reviews of user privileges]
578		REFERENCES
579		Source Assessment Procedures: <u>AC-06</u> , <u>AC-06(01)</u> , <u>AC-06(07)</u> , <u>AU-09(04)</u>
580	3.1.6.	Least Privilege – Privileged Accounts
581		REQUIREMENT: 03.01.06
582		ASSESSMENT OBJECTIVE
583		Determine if:
584 585		A.03.01.06.ODP[01]: personnel or roles to which privileged accounts on the system are to be restricted are defined.
586 587		A.03.01.06.a: privileged accounts on the system are restricted to <a.03.01.06.odp[01]: or="" personnel="" roles="">.</a.03.01.06.odp[01]:>
588 589		A.03.01.06.b: users (or roles) with privileged accounts are required to use non-privileged accounts when accessing nonsecurity functions or nonsecurity information.
590		ASSESSMENT METHODS AND OBJECTS
591		Francisco
391		Examine
592 593 594 595 596		[SELECT FROM: access control policy and procedures; procedures for least privilege; list of system-generated privileged accounts; list of system administration personnel; system audit records; system configuration settings; system security plan; list of system-generated security functions or security-relevant information assigned to system accounts or roles; other relevant documents or records]
592 593 594 595		[SELECT FROM: access control policy and procedures; procedures for least privilege; list of system-generated privileged accounts; list of system administration personnel; system audit records; system configuration settings; system security plan; list of system-generated security functions or security-relevant information assigned to system accounts or roles; other relevant
592 593 594 595 596		[SELECT FROM: access control policy and procedures; procedures for least privilege; list of system-generated privileged accounts; list of system administration personnel; system audit records; system configuration settings; system security plan; list of system-generated security functions or security-relevant information assigned to system accounts or roles; other relevant documents or records]
592 593 594 595 596 597		[SELECT FROM: access control policy and procedures; procedures for least privilege; list of system-generated privileged accounts; list of system administration personnel; system audit records; system configuration settings; system security plan; list of system-generated security functions or security-relevant information assigned to system accounts or roles; other relevant documents or records] Interview [SELECT FROM: personnel with responsibilities for defining least privileges; personnel with
592 593 594 595 596 597 598 599		[SELECT FROM: access control policy and procedures; procedures for least privilege; list of system-generated privileged accounts; list of system administration personnel; system audit records; system configuration settings; system security plan; list of system-generated security functions or security-relevant information assigned to system accounts or roles; other relevant documents or records] Interview [SELECT FROM: personnel with responsibilities for defining least privileges; personnel with information security responsibilities; system administrators]
592 593 594 595 596 597 598 599 600		[SELECT FROM: access control policy and procedures; procedures for least privilege; list of system-generated privileged accounts; list of system administration personnel; system audit records; system configuration settings; system security plan; list of system-generated security functions or security-relevant information assigned to system accounts or roles; other relevant documents or records] Interview [SELECT FROM: personnel with responsibilities for defining least privileges; personnel with information security responsibilities; system administrators] Test
592 593 594 595 596 597 598 599 600		[SELECT FROM: access control policy and procedures; procedures for least privilege; list of system-generated privileged accounts; list of system administration personnel; system audit records; system configuration settings; system security plan; list of system-generated security functions or security-relevant information assigned to system accounts or roles; other relevant documents or records] Interview [SELECT FROM: personnel with responsibilities for defining least privileges; personnel with information security responsibilities; system administrators] Test [SELECT FROM: mechanisms for implementing least privilege functions]
592 593 594 595 596 597 598 599 600 601	3.1.7.	[SELECT FROM: access control policy and procedures; procedures for least privilege; list of system-generated privileged accounts; list of system administration personnel; system audit records; system configuration settings; system security plan; list of system-generated security functions or security-relevant information assigned to system accounts or roles; other relevant documents or records] Interview [SELECT FROM: personnel with responsibilities for defining least privileges; personnel with information security responsibilities; system administrators] Test [SELECT FROM: mechanisms for implementing least privilege functions] REFERENCES
592 593 594 595 596 597 598 599 600 601 602	3.1.7.	[SELECT FROM: access control policy and procedures; procedures for least privilege; list of system-generated privileged accounts; list of system administration personnel; system audit records; system configuration settings; system security plan; list of system-generated security functions or security-relevant information assigned to system accounts or roles; other relevant documents or records] Interview [SELECT FROM: personnel with responsibilities for defining least privileges; personnel with information security responsibilities; system administrators] Test [SELECT FROM: mechanisms for implementing least privilege functions] REFERENCES Source Assessment Procedures: AC-06(02), AC-06(05)
592 593 594 595 596 597 598 599 600 601 602 603	3.1.7.	[SELECT FROM: access control policy and procedures; procedures for least privilege; list of system-generated privileged accounts; list of system administration personnel; system audit records; system configuration settings; system security plan; list of system-generated security functions or security-relevant information assigned to system accounts or roles; other relevant documents or records] Interview [SELECT FROM: personnel with responsibilities for defining least privileges; personnel with information security responsibilities; system administrators] Test [SELECT FROM: mechanisms for implementing least privilege functions] REFERENCES Source Assessment Procedures: AC-06(02), AC-06(05) Least Privilege – Privileged Functions

608 A.03.01.07.a: non-privileged users are prevented from executing privileged functions. 609 **A.03.01.07.b:** the execution of privileged functions is logged. 610 ASSESSMENT METHODS AND OBJECTS 611 **Examine** 612 [SELECT FROM: access control policy and procedures; procedures for least privilege; system 613 design documentation; system configuration settings; system audit records; list of audited events; 614 list of privileged functions to be audited and associated user account assignments; system 615 security plan; other relevant documents or records] 616 Interview 617 [SELECT FROM: personnel with responsibilities for reviewing least privileges; personnel with information security responsibilities; system developers; system administrators] 618 619 **Test** 620 [SELECT FROM: mechanisms for auditing the execution of least privilege functions; mechanisms 621 for implementing least privilege functions for non-privileged users] 622 REFERENCES 623 Source Assessment Procedures: AC-06(09), AC-06(10) 624 3.1.8. Unsuccessful Logon Attempts 625 **REQUIREMENT: 03.01.08** 626 **ASSESSMENT OBJECTIVE** 627 Determine if: 628 A.03.01.08.ODP[01]: the number of consecutive invalid logon attempts by a user allowed 629 during a time period is defined. 630 A.03.01.08.ODP[02]: the time period to which the number of consecutive invalid logon 631 attempts by a user is limited is defined. A.03.01.08: the number of consecutive invalid logon attempts by a user during 632 633 <03.01.08.ODP[02]: time period> is limited to <A.03.01.08.ODP[01]: number>. 634 **ASSESSMENT METHODS AND OBJECTS** 635 **Examine** 636 [SELECT FROM: access control policy and procedures; procedures for unsuccessful logon 637 attempts: system design documentation: system audit records; system configuration settings: 638 system security plan: other relevant documents or records] 639 Interview 640 [SELECT FROM: personnel with information security responsibilities; system developers; system 641 administrators] 642 Test 643 ISELECT FROM: mechanisms for implementing the access control policy for unsuccessful logon 644 attempts1

645		REFERENCES
646		Source Assessment Procedure: AC-07
647	3.1.9.	System Use Notification
648		REQUIREMENT: 03.01.09
649		ASSESSMENT OBJECTIVE
650		Determine if:
651 652		A.03.01.09: a system use notification message with privacy and security notices consistent with applicable CUI rules is displayed before granting access to the system.
653		ASSESSMENT METHODS AND OBJECTS
654		Examine
655 656 657 658 659		[SELECT FROM: access control policy and procedures; privacy and security policies, procedures for system use notification; documented approval of system use notification messages; system audit records; user acknowledgements of system use notification messages; system design documentation; system configuration settings; system use notification messages; system security plan; other relevant documents or records]
660		Interview
661 662		[SELECT FROM: personnel with information security responsibilities; legal counsel; system developers; system administrators]
663		Test
664		[SELECT FROM: mechanisms for implementing system use notifications]
665		REFERENCES
666		Source Assessment Procedure: <u>AC-08</u>
667	3.1.10). Device Lock
668		REQUIREMENT: 03.01.10
669		ASSESSMENT OBJECTIVE
670		Determine if:
671 672 673		A.03.01.10.ODP[01]: one or more of the following parameter values is/are selected: {initiating a device lock after <a.03.01.10.odp[02] period="" time=""> of inactivity; requiring the user to initiate a device lock before leaving the system unattended}.</a.03.01.10.odp[02]>
674 675		A.03.01.10.ODP[02]: time period of inactivity after which a device lock is initiated is defined (if selected).
676 677		A.03.01.10.a: access to the system is prevented by <a.03.01.10.odp[01]: parameter="" selected="" value(s)="">.</a.03.01.10.odp[01]:>
678 679		A.03.01.10.b: the device lock is retained until the user reestablishes access using established identification and authentication procedures.
680 681		A.03.01.10.c: information previously visible on the display is concealed via device lock with a publicly viewable image.

682		ASSESSMENT METHODS AND OBJECTS
683		Examine
684 685 686 687		[SELECT FROM: access control policy and procedures; procedures for session lock and identification and authentication; system design documentation; system configuration settings; display screen with session lock activated; system security plan; other relevant documents or records]
688		Interview
689 690		[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]
691		Test
692 693		[SELECT FROM: mechanisms for implementing the access control policy for session lock; session lock mechanisms]
694		REFERENCES
695		Source Assessment Procedures: <u>AC-11</u> , <u>AC-11(01)</u>
696	3.1.11.	Session Termination
697		REQUIREMENT: 03.01.11
698		ASSESSMENT OBJECTIVE
699		Determine if:
700 701		A.03.01.11.ODP[01]: conditions or trigger events that require session disconnect are defined.
702 703		A.03.01.11: a user session is automatically terminated after <a.03.01.11.odp[01]: conditions="" events="" or="" trigger="">.</a.03.01.11.odp[01]:>
704		ASSESSMENT METHODS AND OBJECTS
705		Examine
706 707 708 709		[SELECT FROM: access control policy and procedures; procedures for session termination; system design documentation; system configuration settings; list of conditions or trigger events requiring session disconnect; system audit records; system security plan; other relevant documents or records]
710		Interview
711 712		[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]
713		Test
714		[SELECT FROM: automated mechanisms for implementing user session termination]
715		REFERENCES
716		Source Assessment Procedure: <u>AC-12</u>
717	3.1.12.	Remote Access
718		REQUIREMENT: 03.01.12

719		ASSESSMENT OBJECTIVE
720		Determine if:
721		A.03.01.12.a[01]: types of allowable remote system access are defined.
722 723		A.03.01.12.a[02]: usage restrictions are established for each type of allowable remote system access.
724 725		A.03.01.12.a[03]: configuration requirements are established for each type of allowable remote system access.
726 727		A.03.01.12.a[04]: connection requirements are established for each type of allowable remote system access.
728 729		A.03.01.12.b: each type of remote system access is authorized prior to establishing such connections.
730		A.03.01.12.c: remote access to the system is routed through managed access control points.
731		A.03.01.12.d[1]: remote execution of privileged commands is authorized.
732		A.03.01.12.d[2]: remote access to security-relevant information is authorized.
733		ASSESSMENT METHODS AND OBJECTS
734		Examine
735 736 737 738 739 740		[SELECT FROM: access control policy and procedures; procedures for remote system access; remote system access configuration and connection requirements; configuration management plan; system configuration settings; remote access authorizations; system audit records; system design documentation; procedures for remote access to the system; system monitoring records; list of managed network access control points; system security plan; other relevant documents or records]
741		Interview
742 743		[SELECT FROM: personnel with responsibilities for managing remote access connections; personnel with information security responsibilities; system administrators]
744		Test
745 746 747		[SELECT FROM: mechanisms for monitoring and controlling remote access methods; mechanisms for routing remote accesses through managed access control points; remote access management capability for the system]
748		REFERENCES
749		Source Assessment Procedures: AC-17, AC-17(03), AC-17(04)
750	3.1.13.	Withdrawn
751		Incorporated into <u>03.01.12</u> .
752	3.1.14.	Withdrawn
753		Incorporated into <u>03.01.12</u> .
754	3.1.15.	Withdrawn
755		Incorporated into 03.01.12.

756	3.1.16.	Wireless Access
757		REQUIREMENT: 03.01.16
758		ASSESSMENT OBJECTIVE
759		Determine if:
760		A.03.01.16.a[01]: each type of wireless access to the system is defined.
761 762		A.03.01.16.a[02]: usage restrictions are established for each type of wireless access to the system.
763 764		A.03.01.16.a[03]: configuration requirements are established for each type of wireless access to the system.
765 766		A.03.01.16.a[04]: connection requirements are established for each type of wireless access to the system.
767 768		A.03.01.16.b: each type of wireless access to the system is authorized prior to establishing such connections.
769 770		A.03.01.16.c: wireless networking capabilities not intended for use are disabled prior to issuance and deployment.
771		ASSESSMENT METHODS AND OBJECTS
772		Examine
773 774 775 776		[SELECT FROM: access control policy and procedures; procedures for wireless system access; wireless system access configuration and connection requirements; configuration management plan; system configuration settings; wireless access authorizations; system audit records; system design documentation; system security plan; other relevant documents or records]
777		Interview
778 779		[SELECT FROM: personnel with responsibilities for managing wireless access connections; personnel with information security responsibilities; system developers; system administrators]
780		Test
781 782 783		[SELECT FROM: wireless access management capability for the system; mechanisms for implementing wireless access protections to the system; mechanisms for managing the disabling of wireless networking capabilities]
784		REFERENCES
785		Source Assessment Procedures: AC-18, AC-18(03)
786	3.1.17.	Withdrawn
787		Incorporated into <u>03.01.16</u> .
788	3.1.18.	Access Control for Mobile Devices
789		REQUIREMENT: 03.01.18
790		ASSESSMENT OBJECTIVE
791		Determine if:

792 A.03.01.18.a[01]: usage restrictions are established for mobile devices. 793 A.03.01.18.a[02]: configuration requirements are established for mobile devices. 794 A.03.01.18.a[03]: connection requirements are established for mobile devices. 795 **A.03.01.18.b**: the connection of mobile devices to the system is authorized. 796 A.03.01.18.c: full-device or container-based encryption is implemented to protect the 797 confidentiality of CUI on mobile devices. 798 ASSESSMENT METHODS AND OBJECTS 799 **Examine** 800 [SELECT FROM: access control policy and procedures; procedures for mobile device access 801 control; system design documentation; configuration management plan; system configuration 802 settings; authorizations for mobile device connections to organizational systems; system audit 803 records; encryption mechanisms and associated configuration documentation; system security 804 plan; other relevant documents or records] 805 Interview 806 [SELECT FROM: personnel with access control responsibilities for mobile devices; personnel 807 using mobile devices to access organizational systems; personnel with information security 808 responsibilities; system administrators] 809 **Test** 810 [SELECT FROM: access control capability for mobile device connections to organizational 811 systems; encryption mechanisms for protecting the confidentiality of CUI on mobile devices; 812 configurations of mobile devices] 813 REFERENCES 814 Source Assessment Procedures: AC-19, AC-19(05) 815 3.1.19. Withdrawn Incorporated into 03.01.18. 816 817 3.1.20. Use of External Systems 818 **REQUIREMENT: 03.01.20** 819 **ASSESSMENT OBJECTIVE** 820 Determine if: 821 A.03.01.20.ODP[01]: terms and conditions to be satisfied on external systems prior to 822 allowing the use of or access to those systems by authorized individuals are defined. 823 A.03.01.20.ODP[02]: security requirements to be satisfied on external systems prior to 824 allowing the use of or access to those systems by authorized individuals are defined. 825 A.03.01.20.a: the use of external systems is prohibited unless the systems are specifically 826 authorized. 827 A.03.01.20.b[01]: the following terms and conditions to be satisfied on external systems prior to 828 allowing the use of or access to those systems by authorized individuals are established: 829 <A.03.01.20.ODP[01]: terms and conditions>.

830 831 832		A.03.01.20.b[02]: the following security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are established: < A.03.01.20.ODP[02]: security requirements>.
833 834 835 836		A.03.01.20.c.01: authorized individuals are permitted to use an external system to access the organizational system or to process, store, or transmit CUI only after verification of the implementation of security requirements on the external system as specified in the organization's security plans.
837 838 839 840		A.03.01.20.c.02: authorized individuals are permitted to use an external system to access the organizational system or to process, store, or transmit CUI only after the retention of approved system connection or processing agreements with the organizational entity hosting the external system.
841 842		A.03.01.20.d: the use of organization-controlled portable storage devices by authorized individuals on external systems is restricted.
843		ASSESSMENT METHODS AND OBJECTS
844		Examine
845 846 847 848		[SELECT FROM: access control policy and procedures; procedures for the use of external systems; terms and conditions for the use of external systems; external systems security requirements; list of types of applications accessible from external systems; system configuration settings; system security plan; other relevant documents or records]
849		Interview
850 851 852		[SELECT FROM: personnel with responsibilities for defining terms, conditions, and security requirements for the use of external systems; personnel with information security responsibilities; system administrators]
853		Test
854 855		[SELECT FROM: mechanisms for implementing and/or enforcing terms, conditions, and security requirements for the use of external systems]
856		REFERENCES
857		Source Assessment Procedures: AC-20, AC-20(01), AC-20(02)
858	3.1.21.	Withdrawn
859		Incorporated into <u>03.01.20</u> .
860	3.1.22.	Publicly Accessible Content
861		REQUIREMENT: 03.01.22
862		ASSESSMENT OBJECTIVE
863		Determine if:
864 865		A.03.01.22.a: authorized individuals are trained to ensure that publicly accessible information does not contain CUI.
866		A.03.01.22.b[01]: the content on publicly accessible systems is periodically reviewed for CUI.
867		A.03.01.22.b[02]: CUI is removed from publicly accessible systems if discovered.

868	ASSESSMENT METHODS AND OBJECTS	
869	Examine	
870 871 872 873 874	[SELECT FROM: access control policy and procedures; procedures for publicly accessible content; list of users authorized to post publicly accessible content on organizational syste training materials and/or records; records of publicly accessible information reviews; record response to CUI discovered on public websites; system audit logs; security awareness trained records; system security plan; other relevant documents or records]	ms; ds of
875	Interview	
876 877	[SELECT FROM: personnel with responsibilities for managing publicly accessible informat posted on organizational systems; personnel with information security responsibilities]	ion
878	Test	
879 880	[SELECT FROM: mechanisms for implementing the management of publicly accessible content]	
881	REFERENCES	
882	Source Assessment Procedure: AC-22	
883	3.2. Awareness and Training	
884	3.2.1. Literacy Training and Awareness	
885	REQUIREMENT: 03.02.01	
886	ASSESSMENT OBJECTIVE	
887	Determine if:	
888	A.03.02.01.ODP[01]: events that require role-based security training are defined.	
889 890	A.03.02.01.a.01[01]: security literacy training is provided to system users as part of initial traffer new users.	aining
891 892	A.03.02.01.a.01[02]: security literacy training is provided to system users periodically after i training.	nitial
893 894	A.03.02.01.a.02: security literacy training is provided to system users when required by system changes or following <a.03.02.01.odp[01] events="">.</a.03.02.01.odp[01]>	em
895 896	A.03.02.01.a.03[01]: security literacy training on recognizing indicators of insider threat is provided.	
897	A.03.02.01.a.03[02]: security literacy training on reporting indicators of insider threat is prov	ided.
898 899	A.03.02.01.a.03[03]: security literacy training on recognizing indicators of social engineering provided.	j is
900 901	A.03.02.01.a.03[04]: security literacy training on reporting indicators of social engineering is provided.	
902 903	A.03.02.01.a.03[05]: security literacy training on recognizing indicators of social mining is provided.	
904	A.03.02.01.a.03[06]: security literacy training on reporting indicators of social mining is prov	ided.
905	A.03.02.01.b[01]: security literacy training content is updated periodically.	

906 A.03.02.01.b[02]: security literacy training content is updated following < A.03.02.01.ODP[01] 907 events>. 908 ASSESSMENT METHODS AND OBJECTS 909 **Examine** 910 [SELECT FROM: security literacy training and awareness policy and procedures; procedures for 911 security literacy training and awareness implementation; codes of federal regulations; security 912 literacy and awareness training curriculum; security literacy and awareness training materials; 913 training records; system security plan; other relevant documents or records] 914 Interview 915 [SELECT FROM: personnel with responsibilities for security literacy training and awareness; 916 personnel comprising the general system user community; personnel with information security 917 responsibilities] 918 **Test** 919 [SELECT FROM: mechanisms for managing information security literacy training and awareness] 920 **REFERENCES** 921 Source Assessment Procedures: AT-02, AT-02(02), AT-02(03) 922 3.2.2. Role-Based Training 923 REQUIREMENT: 03.02.02 924 **ASSESSMENT OBJECTIVE** 925 Determine if: 926 A.03.02.02.ODP[01]: events that require role-based security training are defined. 927 A.03.02.02.a.01[01]: role-based security training is provided to organizational personnel before 928 authorizing access to the system or CUI. 929 A.03.02.02.a.01[02]: role-based security training is provided to organizational personnel before 930 performing assigned duties. 931 A.03.02.02.a.01[03]: role-based security training is provided to organizational personnel 932 periodically after initial access. 933 A.03.02.02.a.02: role-based security training is provided to organizational personnel when 934 required by system changes or following < A.03.02.02.0DP[01] events>. 935 A.03.02.02.b[01]: role-based training content is updated periodically. 936 A.03.02.02.b[02]: role-based training content is updated following < A.03.02.02.ODP[01] 937 events>. 938 **ASSESSMENT METHODS AND OBJECTS** 939 **Examine** 940 [SELECT FROM: security awareness and training policy and procedures; procedures for security 941 training implementation; codes of federal regulations; security training curriculum; security training 942 materials; training records; system security plan; other relevant documents or records]

943		Interview
944 945		[SELECT FROM: personnel with responsibilities for role-based security training; personnel with assigned system security roles and responsibilities]
946		Test
947		[SELECT FROM: mechanisms for managing role-based security training and awareness]
948		REFERENCES
949		Source Assessment Procedure: <u>AT-03</u>
950	3.2.3.	Withdrawn
951		Incorporated into <u>03.02.01</u> .
952	3.3.	Audit and Accountability
953	3.3.1.	Event Logging
954		REQUIREMENT: 03.03.01
955		ASSESSMENT OBJECTIVE
956		Determine if:
957		A.03.03.01.ODP[01]: the event types selected for logging within the system are defined.
958 959		A.03.03.01.a: the following event types are specified for logging within the system: <a.03.03.01.odp[01] event="" types="">.</a.03.03.01.odp[01]>
960		A.03.03.01.b[01]: the event types selected for logging are reviewed periodically.
961		A.03.03.01.b[02]: the event types selected for logging are updated periodically.
962		ASSESSMENT METHODS AND OBJECTS
963		Examine
964 965 966		[SELECT FROM: audit and accountability policy and procedures; procedures for auditable events; system design documentation; system configuration settings; system audit records; system auditable events; system security plan; other relevant documents or records]
967		Interview
968 969		[SELECT FROM: personnel with audit and accountability responsibilities; personnel with information security responsibilities; system administrators]
970		Test
971		[SELECT FROM: mechanisms for implementing system auditing]
972		REFERENCES
973		Source Assessment Procedure: <u>AU-02</u>
974	3.3.2.	Audit Record Content
975		REQUIREMENT: 03.03.02

976		ASSESSMENT OBJECTIVE
977		Determine if:
978		A.03.03.02.a.01: audit records contain information that establishes what type of event occurred.
979		A.03.03.02.a.02: audit records contain information that establishes when the event occurred.
980		A.03.03.02.a.03: audit records contain information that establishes where the event occurred.
981		A.03.03.02.a.04: audit records contain information that establishes the source of the event.
982		A.03.03.02.a.05: audit records contain information that establishes the outcome of the event.
983 984		A.03.03.02.a.06: audit records contain information that establishes the identity of the individuals, subjects, objects, or entities associated with the event.
985		A.03.03.02.b: additional information for audit records is provided, as needed.
986		ASSESSMENT METHODS AND OBJECTS
987		Examine
988 989 990 991		[SELECT FROM: audit and accountability policy and procedures; procedures for the content of audit records; list of organization-defined auditable events; system design documentation; system configuration settings; system audit records; system incident reports; system security plan; other relevant documents or records]
992		Interview
993 994		[SELECT FROM: personnel with audit and accountability responsibilities; personnel with information security responsibilities; system developers; system administrators]
995		Test
996 997		[SELECT FROM: mechanisms for implementing system auditing of auditable events; system audit capability]
998		REFERENCES
999		Source Assessment Procedures: <u>AU-03</u> , <u>AU-03(01)</u>
1000	3.3.3.	Audit Record Generation
1001		REQUIREMENT: 03.03.03
1002		ASSESSMENT OBJECTIVE
1003		Determine if:
1004 1005		A.03.03.03.a: audit records for the selected event types and audit record content specified in 3.3.1 and 3.3.2 are generated.
1005		A.03.03.03.b: audit records are retained for a time period consistent with records retention policy.
1007		ASSESSMENT METHODS AND OBJECTS
1008		Examine
1009 1010 1011		[SELECT FROM: audit and accountability policy and procedures; procedures for audit record generation; system design documentation; list of auditable events; audit records; audit record retention policy and procedures; organization-defined retention period for audit records; audit

1012 1013		record archives; system configuration settings; system security plan; other relevant documents or records]
1014		Interview
1015 1016 1017		[SELECT FROM: personnel with audit record generation responsibilities; personnel with audit record retention responsibilities; personnel with information security responsibilities; system developers; system administrators]
1018		Test
1019		[SELECT FROM: mechanisms for implementing the audit record generation capability]
1020		REFERENCES
1021		Source Assessment Procedures: <u>AU-11</u> , <u>AU-12</u>
1022	3.3.4.	Response to Audit Logging Process Failures
1023		REQUIREMENT: 03.03.04
1024		ASSESSMENT OBJECTIVE
1025		Determine if:
1026 1027		A.03.03.04.ODP[01]: time period for organizational personnel or roles receiving audit logging process failure alerts is defined.
1028 1029		A.03.03.04.ODP[02]: additional actions to be taken in the event of an audit logging process failure are defined.
1030 1031		A.03.03.04.a: organizational personnel or roles are alerted in the event of an audit logging process failure within < <i>A.03.03.04.ODP[01] time period</i> > .
1032 1033		A.03.03.04.b: the following additional actions are taken in the event of an audit logging process failure: < <i>A.03.03.04.ODP[02]</i> additional actions>.
1034		ASSESSMENT METHODS AND OBJECTS
1035		Examine
1036 1037 1038 1039		[SELECT FROM: audit and accountability policy and procedures; procedures for responding to audit processing failures; system design documentation; system configuration settings; list of personnel to be notified in case of an audit processing failure; system audit records; system security plan; other relevant documents or records]
1040		Interview
1041 1042		[SELECT FROM: personnel with audit and accountability responsibilities; personnel with information security responsibilities; system developers; system administrators]
1043		Test
1044		[SELECT FROM: mechanisms for implementing system response to audit processing failures]
1045		REFERENCES
1046		Source Assessment Procedure: <u>AU-05</u>
1047	3.3.5.	Audit Record Review, Analysis, and Reporting
1048		REQUIREMENT: 03.03.05

1049		ASSESSMENT OBJECTIVE
1050		Determine if:
1051 1052		A.03.03.05.a: system audit records are reviewed and analyzed periodically for indications and potential impacts of inappropriate or unusual activity.
1053		A.03.03.05.b: findings are reported to organizational personnel or roles.
1054 1055		A.03.03.05.c: audit records across different repositories are analyzed and correlated to gain organization-wide situational awareness.
1056		ASSESSMENT METHODS AND OBJECTS
1057		Examine
1058 1059 1060 1061 1062		[SELECT FROM: audit and accountability policy and procedures; procedures for audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews and analyses of audit records; system design documentation; system audit records across different repositories; system configuration settings; system security plan; other relevant documents or records]
1063		Interview
1064 1065		[SELECT FROM: personnel with audit review, analysis, and reporting responsibilities; personnel with information security responsibilities]
1066		Test
1067		[SELECT FROM: mechanisms for supporting the analysis and correlation of audit records]
1068		REFERENCES
1069		Source Assessment Procedures: <u>AU-06</u> , <u>AU-06(03)</u>
1070	3.3.6.	Audit Record Reduction and Report Generation
1071		REQUIREMENT: 03.03.06
1072		ASSESSMENT OBJECTIVE
1073		Determine if:
1074 1075 1076		A.03.03.05.a: an audit record reduction and report generation capability that supports audit record review, analysis, reporting requirements, and after-the-fact investigations of incidents is implemented.
1077		A.03.03.05.b: the original content and time ordering of audit records are preserved.
1078		ASSESSMENT METHODS AND OBJECTS
1079		Examine
1080 1081 1082 1083		[SELECT FROM: audit and accountability policy and procedures; procedures for audit reduction and report generation; system design documentation; system configuration settings; system audit records; audit reduction, review, analysis, and reporting tools; system security plan; other relevant documents or records]
1084		Interview
1085 1086		[SELECT FROM: personnel with audit reduction and report generation responsibilities; personnel with information security responsibilities]

1087		Test
1088		[SELECT FROM: audit reduction and report generation capability]
1089		REFERENCES
1090		Source Assessment Procedure: <u>AU-07</u>
1091	337	Time Stamps
1092	0.0.7.	REQUIREMENT: 03.03.07
1093		ASSESSMENT OBJECTIVE
1094		Determine if:
1095 1096		A.03.03.07.ODP[01]: the granularity of time measurement for audit record time stamps is defined.
1097		A.03.03.07.a: internal system clocks are used to generate time stamps for audit records.
1098 1099		A.03.03.07.b[01]: time stamps for audit records meet < A.03.03.07.ODP[01] granularity of time measurement>.
1100 1101 1102		A.03.03.07.b[02]: time stamps for audit records use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp are recorded.
1103		ASSESSMENT METHODS AND OBJECTS
1104		Examine
1105 1106 1107		[SELECT FROM: audit and accountability policy and procedures; procedures for timestamp generation; system design documentation; system configuration settings; system audit records; system security plan; other relevant documents or records]
1108		Interview
1109 1110		[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]
1111		Test
1112		[SELECT FROM: mechanisms for implementing timestamp generation]
1113		REFERENCES
1114		Source Assessment Procedure: <u>AU-08</u>
1115	3.3.8.	Protection of Audit Information
1116		REQUIREMENT: 03.03.08
1117		ASSESSMENT OBJECTIVE
1118		Determine if:
1119 1120		A.03.03.08.a: audit information and audit logging tools are protected from unauthorized access, modification, and deletion.
1121 1122		A.03.03.08.b: access to the management of audit logging functionality is authorized to only a subset of privileged users or roles.

1123		ASSESSMENT METHODS AND OBJECTS
1124		Examine
1125 1126 1127 1128 1129		[SELECT FROM: audit and accountability policy and procedures; access control policy and procedures; procedures for the protection of audit information; system configuration settings; system audit records; audit tools; system-generated list of privileged users with access to the management of audit functionality; access authorizations; access control list; system design documentation; system security plan; other relevant documents or records]
1130		Interview
1131 1132		[SELECT FROM: personnel with audit and accountability responsibilities; personnel with information security responsibilities; system developers; system administrators]
1133		Test
1134 1135		[SELECT FROM: mechanisms for implementing audit information protection; mechanisms for managing access to audit functionality]
1136		REFERENCES
1137		Source Assessment Procedures: <u>AU-09</u> , <u>AU-09(04)</u>
1138	3.3.9.	Withdrawn
1139		Incorporated into <u>03.03.08</u> .
1140	3.4.	Configuration Management
1141	3.4.1.	Baseline Configuration
1142		REQUIREMENT: 03.04.01
1143		ASSESSMENT OBJECTIVE
1144		Determine if:
1145		A.03.04.01.a[01]: a current baseline configuration of the system is developed.
1146 1147		A.03.04.01.a[02]: a current baseline configuration of the system is maintained under configuration control.
1148		A.03.04.01.b[01]: the baseline configuration of the system is reviewed periodically.
1149 1150		A.03.04.01.b[02]: the baseline configuration of the system is reviewed when system components are installed or modified.
1151		A.03.04.01.b[03]: the baseline configuration of the system is updated periodically.
1152 1153		A.03.04.01.b[04]: the baseline configuration of the system is updated when system components are installed or modified.
1154		ASSESSMENT METHODS AND OBJECTS
1155		Examine
1156 1157		[SELECT FROM: configuration management policy and procedures; procedures for the baseline system configuration; configuration management plan; enterprise architecture; system design

1158 1159		documentation; system architecture; system configuration settings; system component inventory change control records; system security plan; other relevant documents or records]
1160		Interview
1161 1162		[SELECT FROM: personnel with configuration management responsibilities; personnel with information security responsibilities; system administrators]
1163		Test
1164 1165		[SELECT FROM: processes for managing baseline configurations; mechanisms for supporting configuration control of the baseline configuration]
1166		REFERENCES
1167		Source Assessment Procedure: <u>CM-02</u>
1168	3.4.2.	Configuration Settings
1169		REQUIREMENT: 03.04.02
1170		ASSESSMENT OBJECTIVE
1171		Determine if:
1172 1173		A.03.04.02.ODP[01]: configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are defined.
1174 1175 1176		A.03.04.02.a[01]: the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are established and documented: <A.03.04.02.ODP[01] configuration settings> .
1177 1178		A.03.04.02.a[02]: the following configuration settings for the system are implemented: <a.03.04.02.odp[01] configuration="" settings="">.</a.03.04.02.odp[01]>
1179 1180		A.03.04.02.b[01]: any deviations from established configuration settings are identified and documented.
1181		A.03.04.02.b[02]: any deviations from established configuration settings are approved.
1182		ASSESSMENT METHODS AND OBJECTS
1183		Examine
1184 1185 1186 1187 1188 1189		[SELECT FROM: configuration management policy and procedures; procedures for system configuration settings; configuration management plan; system design documentation; system configuration settings; common secure configuration checklists; system component inventory; evidence supporting approved deviations from established configuration settings; change control records; system data processing and retention permissions; system audit records; system security plan; other relevant documents or records]
1190		Interview
1191 1192		[SELECT FROM: personnel with security configuration management responsibilities; personnel with information security responsibilities; system administrators]
1193		Test
1194 1195 1196		[SELECT FROM: processes for managing configuration settings; mechanisms that implement, monitor, and/or control system configuration settings; mechanisms that identify and/or document deviations from established configuration settings]

1197		REFERENCES
1198		Source Assessment Procedure: CM-06
1199	3.4.3.	Configuration Change Control
1200		REQUIREMENT: 03.04.03
1201		ASSESSMENT OBJECTIVE
1202		Determine if:
1203		A.03.04.03.a: the types of changes to the system that are configuration-controlled are defined.
1204		A.03.04.03.b[01]: proposed configuration-controlled changes to the system are reviewed.
1205 1206		A.03.04.03.b[02]: proposed configuration-controlled changes to the system are approved or disapproved with explicit consideration for security impacts.
1207		A.03.04.03.c[01]: approved configuration-controlled changes to the system are implemented.
1208		A.03.04.03.c[02]: approved configuration-controlled changes to the system are documented.
1209 1210		A.03.04.03.d[01]: activities associated with configuration-controlled changes to the system are monitored.
1211 1212		A.03.04.03.d[02]: activities associated with configuration-controlled changes to the system are reviewed.
1213		ASSESSMENT METHODS AND OBJECTS
1214		Examine
1215 1216 1217 1218 1219		[SELECT FROM: configuration management policy and procedures; procedures for system configuration change control; configuration management plan; system architecture; configuration settings; change control records; system audit records; change control audit and review reports; agenda, minutes, and documentation from configuration change control oversight meetings; system security plan; other relevant documents or records]
1220		Interview
1221 1222 1223		[SELECT FROM: personnel with configuration change control responsibilities; personnel with information security responsibilities; members of change control board or similar; system administrators]
1224		Test
1225 1226		[SELECT FROM: processes for configuration change control; mechanisms that implement configuration change control]
1227		REFERENCES
1228		Source Assessment Procedure: <u>CM-03</u>
1229	3.4.4.	Impact Analyses
1230		REQUIREMENT: 03.04.04
1231		ASSESSMENT OBJECTIVE
1232		Determine if:

1233		A.03.04.04: changes to the system are analyzed for security impact prior to implementation.
1234		ASSESSMENT METHODS AND OBJECTS
1235		Examine
1236 1237 1238 1239		[SELECT FROM: configuration management policy and procedures; procedures for security impact analyses for system changes; configuration management plan; security impact analysis documentation; system design documentation; analysis tools and outputs; change control records; system audit records; system security plan; other relevant documents or records]
1240		Interview
1241 1242 1243		[SELECT FROM: personnel with security impact analysis responsibilities; personnel with information security responsibilities; members of change control board; system developers; system administrators]
1244		Test
1245		[SELECT FROM: processes for security impact analyses]
1246		REFERENCES
1247		Source Assessment Procedure: <u>CM-04</u>
1248	3.4.5.	Access Restrictions for Change
1249		REQUIREMENT: 03.04.05
1250		ASSESSMENT OBJECTIVE
1251		Determine if:
1252 1253		A.03.04.05[01]: physical access restrictions associated with changes to the system are defined and documented.
1254 1255		A.03.04.05[02]: physical access restrictions associated with changes to the system are approved.
1256		A.03.04.05[03]: physical access restrictions associated with changes to the system are enforced
1257 1258		A.03.04.05[04]: logical access restrictions associated with changes to the system are defined and documented.
1259		A.03.04.05[05]: logical access restrictions associated with changes to the system are approved.
1260		A.03.04.05[06]: logical access restrictions associated with changes to the system are enforced.
1261		ASSESSMENT METHODS AND OBJECTS
1262		Examine
1263 1264 1265 1266 1267		[SELECT FROM: configuration management policy and procedures; procedures for access restrictions for system changes; configuration management plan; system design documentation; system architecture; system configuration settings; logical access approvals; physical access approvals; access credentials; change control records; system audit records; system security plan; other relevant documents or records]
1268		Interview
1269 1270 1271		[SELECT FROM: personnel with logical access control responsibilities; personnel with physical access control responsibilities; personnel with information security responsibilities; system administrators]

1272		Test
1273 1274		[SELECT FROM: processes for managing access restrictions for system changes; mechanisms for supporting, implementing, or enforcing access restrictions associated with system changes]
1275		REFERENCES
1276		Source Assessment Procedure: <u>CM-05</u>
1277	3.4.6.	Least Functionality
1278		REQUIREMENT: 03.04.06
1279		ASSESSMENT OBJECTIVE
1280		Determine if:
1281		A.03.04.06.ODP[01]: functions to be prohibited or restricted are defined.
1282		A.03.04.06.ODP[02]: ports to be prohibited or restricted are defined.
1283		A.03.04.06.ODP[03]: protocols to be prohibited or restricted are defined.
1284		A.03.04.06.ODP[04]: connections to be prohibited or restricted are defined.
1285		A.03.04.06.ODP[05]: services to be prohibited or restricted are defined.
1286		A.03.04.06.ODP[06]: functions deemed unnecessary or non-secure are defined.
1287		A.03.04.06.ODP[07]: ports deemed unnecessary or non-secure are defined.
1288		A.03.04.06.ODP[08]: protocols deemed unnecessary or non-secure are defined.
1289		A.03.04.06.ODP[09]: connections deemed unnecessary or non-secure are defined.
1290		A.03.04.06.ODP[10]: services deemed unnecessary or non-secure are defined.
1291		A.03.04.06.a: the system is configured to provide only mission-essential capabilities.
1292 1293		A.03.04.06.b[01]: the use of the following functions is prohibited or restricted: <a.03.04.06.odp[01]: functions="">.</a.03.04.06.odp[01]:>
1294 1295		A.03.04.06.b[02]: the use of the following ports is prohibited or restricted: <a.03.04.06.odp[02]: ports="">.</a.03.04.06.odp[02]:>
1296 1297		A.03.04.06.b[03]: the use of the following protocols is prohibited or restricted: <a.03.04.06.odp[03]: protocols="">.</a.03.04.06.odp[03]:>
1298 1299		A.03.04.06.b[04]: the use of the following connections is prohibited or restricted: <a.03.04.06.odp[04]: connections="">.</a.03.04.06.odp[04]:>
1300 1301		A.03.04.06.b[05]: the use of the following services is prohibited or restricted: <a.03.04.06.odp[05]: services="">.</a.03.04.06.odp[05]:>
1302 1303		A.03.04.06.c: the system is reviewed periodically to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.
1304 1305		A.03.04.06.d[01]: the following unnecessary or nonsecure functions are disabled or removed: <a.03.04.06.odp[06]: functions="">.</a.03.04.06.odp[06]:>
1306 1307		A.03.04.06.d[02]: the following unnecessary or nonsecure ports are disabled or removed: <a.03.04.06.odp[07]: ports="">.</a.03.04.06.odp[07]:>
1308 1309		A.03.04.06.d[03]: the following unnecessary or nonsecure protocols are disabled or removed: <a.03.04.06.odp[08]: protocols="">.</a.03.04.06.odp[08]:>

1310 1311		A.03.04.06.d[04] : the following unnecessary or nonsecure connections are disabled or removed: <a.03.04.06.odp[09]: connections="">.</a.03.04.06.odp[09]:>
1312 1313		A.03.04.06.d[05]: the following unnecessary or nonsecure services are disabled or removed: < A.03.04.06.ODP[10]: services>.
1314		ASSESSMENT METHODS AND OBJECTS
1315		Examine
1316 1317 1318 1319 1320		[SELECT FROM: configuration management policy and procedures; procedures for least functionality in the system; configuration management plan; system design documentation; system configuration settings; system component inventory; common secure configuration checklists; documented reviews of functions, ports, protocols, and services; change control records; system audit records; system security plan; other relevant documents or records]
1321		Interview
1322 1323 1324		[SELECT FROM: personnel with configuration management responsibilities; personnel with responsibilities for reviewing functions, ports, protocols, and services; personnel with information security responsibilities; system developers; system administrators]
1325		Test
1326 1327 1328 1329		[SELECT FROM: processes for prohibiting or restricting functions, ports, protocols, and services; processes for reviewing or disabling functions, ports, protocols, and services; mechanisms for implementing the review and disabling of functions, ports, protocols, and services; mechanisms for implementing restrictions on or the prohibition of functions, ports, protocols, and services]
1330		REFERENCES
1331		Source Assessment Procedures: <u>CM-07</u> , <u>CM-07(01)</u>
1332	3.4.7.	Withdrawn
1333		Incorporated into <u>03.04.06</u> .
1334	3.4.8.	Authorized Software – Allow by Exception
1335		REQUIREMENT: 03.04.08
1336		ASSESSMENT OBJECTIVE
1337		Determine if:
1338		A.03.04.08.a: software programs authorized to execute on the system are identified.
1339 1340		A.03.04.08.b: a deny-all, allow-by-exception policy for the execution of software programs on the system is implemented.
1341		A.03.04.08.c[01]: the list of authorized software programs is reviewed periodically.
1342		A.03.04.08.c[02]: the list of authorized software programs is updated periodically.
1343		ASSESSMENT METHODS AND OBJECTS
1344		Examine
1345 1346 1347		[SELECT FROM: configuration management policy and procedures; procedures for least functionality in the system; configuration management plan; system design documentation; system configuration settings; list of software programs authorized to execute on the system;

1348 1349 1350	system component inventory; common secure configuration checklists; review and update records associated with list of authorized software programs; change control records; system audit records; system security plan; other relevant documents or records]
1351	Interview
1352 1353	[SELECT FROM: personnel with responsibilities for identifying software authorized to execute on the system; personnel with information security responsibilities; system administrators]
1354	Test
1355 1356 1357	[SELECT FROM: processes for identifying, reviewing, and updating programs authorized to execute on the system; processes for implementing authorized software policy; mechanisms for supporting and/or implementing authorized software policy]
1358	REFERENCES
1359	Source Assessment Procedure: <u>CM-07(05)</u>
1360	3.4.9. Withdrawn
1361	Addressed by <u>03.01.05</u> , <u>03.01.06</u> , <u>03.01.07</u> , and <u>03.04.08</u> .
1362	3.4.10. System Component Inventory
1363	REQUIREMENT: 03.04.10
1364	ASSESSMENT OBJECTIVE
1365	Determine if:
1366	A.03.04.10.a: an inventory of system components is developed and documented.
1367	A.03.04.10.b[01]: the system component inventory is reviewed periodically.
1368	A.03.04.10.b[02]: the system component inventory is updated periodically.
1369 1370	A.03.04.10.c[01]: the system component inventory is updated as part of component installations.
1371	A.03.04.10.c[02]: the system component inventory is updated as part of component removals.
1372	A.03.04.10.c[03]: the system component inventory is updated as part of system updates.
1373	ASSESSMENT METHODS AND OBJECTS
1374	Examine
1375 1376 1377 1378 1379	[SELECT FROM: configuration management policy and procedures; procedures for system component inventory; configuration management plan; system design documentation; system component inventory; inventory reviews and update records; component installation records; change control records; component removal records; system change records; system security plan; other relevant documents or records]
1380	Interview
1381 1382	[SELECT FROM: personnel with component inventory management responsibilities; personnel with information security responsibilities; system administrators]

1383		Test
1384 1385 1386 1387		[SELECT FROM: processes for managing the system component inventory; mechanisms for supporting and/or implementing the system component inventory; processes for updating the system component inventory; mechanisms for supporting and/or implementing the system component inventory updates]
1388		REFERENCES
1389		Source Assessment Procedures: <u>CM-08</u> , <u>CM-08(01)</u>
1390	3.4.11.	Information Location
1391		REQUIREMENT: 03.04.11
1392		ASSESSMENT OBJECTIVE
1393		Determine if:
1394		A.03.04.11.a[01]: the location of CUI is identified and documented.
1395 1396		A.03.04.11.a[02]: the system components on which CUI is processed are identified and documented.
1397 1398		A.03.04.11.a[03]: the system components on which CUI is stored are identified and documented.
1399 1400		A.03.04.11.b[01]: users who have access to the system and system components where CUI is processed are identified and documented.
1401 1402		A.03.04.11.b[02]: users who have access to the system and system components where CUI is stored are identified and documented.
1403 1404		A.03.04.11.c[01]: changes to the location (i.e., system or system components) where CUI is processed are documented.
1405 1406		A.03.04.11.c[02]: changes to the location (i.e., system or system components) where CUI is stored are documented.
1407		ASSESSMENT METHODS AND OBJECTS
1408		Examine
1409 1410 1411 1412 1413		[SELECT FROM: configuration management policy and procedures; configuration management plan; procedures for identification and documentation of information location; system; audit records; architecture documentation; system design documentation; list of users with system and system component access; change control records; system component inventory; system security plan; other relevant documents or records]
1414		Interview
1415 1416 1417		[SELECT FROM: personnel with responsibilities for managing information location and user access; personnel with responsibilities for operating, using, and/or maintaining the system; personnel with information security responsibilities; system developers; system administrators]
1418		Test
1419 1420		[SELECT FROM: processes governing information location; mechanisms for enforcing policies and methods for governing information location]
1421		REFERENCES
1422		Source Assessment Procedure: CM-12

1423	3.4.12.	System and Component Configuration for High-Risk Areas
1424		REQUIREMENT: 03.04.12
1425		ASSESSMENT OBJECTIVE
1426		Determine if:
1427 1428		A.03.04.12.ODP[01]: configurations for systems or system components to be issued to individuals traveling to high-risk locations are defined.
1429 1430		A.03.04.12.ODP[02]: the security requirements to be applied to the system or system components when individuals return from travel are defined.
1431 1432		A.03.04.12.a: systems or system components with the following configurations are issued to individuals traveling to high-risk locations: < <i>A.03.04.12.ODP[01]: configurations</i> >.
1433 1434		A.03.04.12.b: the following security requirements are applied to the system or system components when the individuals return from travel: < <i>A.03.04.12.ODP[02]: requirements</i> >.
1435		ASSESSMENT METHODS AND OBJECTS
1436		Examine
1437 1438 1439 1440 1441 1442		[SELECT FROM: configuration management policy and procedures; configuration management plan; procedures for the baseline configuration of the system; procedures for system component installations and upgrades; system component inventory; system component installations or upgrades and associated records; records of system baseline configuration reviews and updates; system configuration settings; system architecture; change control records; system security plan; other relevant documents or records]
1443		Interview
1444 1445		[SELECT FROM: personnel with configuration management responsibilities; personnel with information security responsibilities; system administrators]
1446		Test
1447		[SELECT FROM: processes for managing baseline configurations]
1448		REFERENCES
1449		Source Assessment Procedure: <u>CM-02(07)</u>
1450	3.5. <u>ld</u>	entification and Authentication
1451	3.5.1.	User Identification, Authentication, and Re-Authentication
1452	ı	REQUIREMENT: 03.05.01
1453	1	ASSESSMENT OBJECTIVE
1454	j	Determine if:
1455		A.03.05.01.ODP[01]: circumstances or situations that require re-authentication are defined.
1456	,	A.03.05.01.a[01]: system users are uniquely identified and authenticated.
1457 1458		A.03.05.01.a[02]: the unique identification of authenticated system users is associated with processes acting on behalf of those users.

1459 A.03.05.01.b: users are reauthenticated when < A.03.05.01.ODP[01]: circumstances or 1460 situations>. 1461 **ASSESSMENT METHODS AND OBJECTS** 1462 **Examine** 1463 [SELECT FROM: identification and authentication policy and procedures; list of circumstances or 1464 situations requiring re-authentication; system design documentation; system configuration 1465 settings; system audit records; list of system accounts; system security plan; other relevant 1466 documents or records] 1467 Interview 1468 [SELECT FROM: personnel with identification and authentication responsibilities; personnel with 1469 system operations responsibilities; personnel with account management responsibilities; system 1470 developers; personnel with information security responsibilities; system administrators] 1471 **Test** 1472 [SELECT FROM: processes for uniquely identifying and authenticating users; mechanisms for 1473 supporting and/or implementing identification and authentication capabilities] 1474 **REFERENCES** 1475 Source Assessment Procedures: IA-02, IA-11 3.5.2. Device Identification and Authentication 1476 1477 **REQUIREMENT: 03.05.02** 1478 **ASSESSMENT OBJECTIVE** 1479 Determine if: 1480 A.03.05.02: devices are uniquely identified and authenticated before establishing a system 1481 connection. 1482 ASSESSMENT METHODS AND OBJECTS 1483 **Examine** 1484 [SELECT FROM: identification and authentication policy and procedures; procedures for device 1485 identification and authentication; system design documentation; list of devices requiring unique 1486 identification and authentication; device connection reports; system configuration settings; system 1487 security plan; other relevant documents or records] 1488 Interview 1489 ISELECT FROM: personnel with responsibilities for device identification and authentication: 1490 personnel with information security responsibilities; system developers; system administrators] 1491 Test 1492 [SELECT FROM: mechanisms for supporting and/or implementing device identification and 1493 authentication capabilities] 1494 REFERENCES 1495 Source Assessment Procedure: IA-03

1496	3.5.3.	Multi-Factor Authentication
1497		REQUIREMENT: 03.05.03
1498		ASSESSMENT OBJECTIVE
1499		Determine if:
1500		A.03.05.03: multi-factor authentication for access to system accounts is implemented.
1501		ASSESSMENT METHODS AND OBJECTS
1502		Examine
1503 1504 1505		[SELECT FROM: identification and authentication policy and procedures; system design documentation; list of system accounts; system configuration settings; system audit records; system security plan; other relevant documents or records]
1506		Interview
1507 1508 1509		[SELECT FROM: personnel with system operations responsibilities; personnel with account management responsibilities; personnel with information security responsibilities; system developers; system administrators]
1510		Test
1511 1512		[SELECT FROM: mechanisms for supporting and/or implementing a multi-factor authentication capability]
1513		REFERENCES
1514		Source Assessment Procedures: <u>IA-02(01)</u> , <u>IA-02(02)</u>
1515	3.5.4.	Replay-Resistant Authentication
1516		REQUIREMENT: 03.05.04
1517		ASSESSMENT OBJECTIVE
1518		Determine if:
1519 1520		A.03.05.04: replay-resistant authentication mechanisms for access to system accounts are implemented.
1521		ASSESSMENT METHODS AND OBJECTS
1522		Examine
1523 1524 1525		[SELECT FROM: identification and authentication policy and procedures; system design documentation; system audit records; system configuration settings; list of privileged system accounts; system security plan; other relevant documents or records]
1526		Interview
1527 1528 1529		[SELECT FROM: personnel with system operations responsibilities; personnel with account management responsibilities; personnel with information security responsibilities; system developers; system administrators]
1530		Test
1531 1532		[SELECT FROM: mechanisms for supporting and/or implementing identification and authentication capabilities; mechanisms for supporting and/or implementing replay-resistance]

1566		REQUIREMENT: 03.05.07
1565	3.5.7.	Password Management
1564	3.5.6.	Withdrawn
1563		Source Assessment Procedures: <u>IA-04</u> , <u>IA-04(04)</u>
1562		REFERENCES
1561		[SELECT FROM: mechanisms for supporting and/or implementing identifier management]
1560		Test
1558 1559		[SELECT FROM: personnel with identifier management responsibilities; personnel with information security responsibilities; system developers; system administrators]
1557		Interview
1555 1556		identifiers generated from physical access control devices; system security plan; other relevant documents or records]
1552 1553 1554		[SELECT FROM: identification and authentication policy and procedures; procedures for identifier management; procedures for account management; system design documentation; list of system accounts; list of characteristics identifying individual status; system configuration settings; list of
1551		Examine
1550		ASSESSMENT METHODS AND OBJECTS
1549		A.03.05.05.d: the status of each individual is uniquely identified with an identifying characteristic.
1548		A.03.05.05.c: the reuse of identifiers for < A.03.05.05.ODP[02]: time period> is prevented.
1546 1547		A.03.05.05.b[02]: an identifier that identifies an individual, group, role, service, or device is assigned.
1544 1545		A.03.05.05.b[01]: an identifier that identifies an individual, group, role, service, or device is selected.
1542 1543		A.03.05.05.a: authorization is received from <A.03.05.05.ODP[01]: personnel or roles> to assign an individual, group, role, service, or device identifier.
1541		A.03.05.05.ODP[02]: a time period for preventing the reuse of identifiers is defined.
1539 1540		A.03.05.05.ODP[01]: personnel or roles from whom authorization must be received to assign an identifier are defined.
1538		Determine if:
1537		ASSESSMENT OBJECTIVE
1536		REQUIREMENT: 03.05.05
1535	3.5.5.	Identifier Management
1534		Source Assessment Procedure: <u>IA-02(08)</u>
1533		REFERENCES

1567		ASSESSMENT OBJECTIVE
1568		Determine if:
1569		A.03.05.07.ODP[01]: password composition and complexity rules are defined.
1570		A.03.05.07.a[01]: a list of commonly used, expected, or compromised passwords is maintained.
1571 1572		A.03.05.07.a[02]: a list of commonly used, expected, or compromised passwords is updated periodically.
1573 1574		A.03.05.07.a[03]: a list of commonly used, expected, or compromised passwords is updated when organizational passwords are suspected to have been compromised.
1575 1576		A.03.05.07.b: passwords are verified not to be found on the list of commonly used, expected, or compromised passwords when they are created or updated by users.
1577		A.03.05.07.c: passwords are only transmitted over cryptographically protected channels.
1578		A.03.05.07.d: passwords are stored in a cryptographically protected form.
1579		A.03.05.07.e: a new password is selected upon first use after account recovery.
1580 1581		A.03.05.07.f : the following composition and complexity rules are enforced: <A.03.05.07.ODP[01] : rules>.
1582		ASSESSMENT METHODS AND OBJECTS
1583		Examine
1584 1585 1586		[SELECT FROM: identification and authentication policy and procedures; password policy; procedures for authenticator management; system design documentation; system configuration settings; password configurations; system security plan; other relevant documents or records]
1587		Interview
1588 1589		[SELECT FROM: personnel with authenticator management responsibilities; personnel with information security responsibilities; system developers; system administrators]
1590		Test
1591 1592		[SELECT FROM: mechanisms for supporting and/or implementing a password-based authenticator management capability]
1593		REFERENCES
1594		Source Assessment Procedure: <u>IA-05(01)</u>
1595	3.5.8.	Withdrawn
1596	3.5.9.	Withdrawn
1597		Incorporated into <u>03.05.07</u> .
1598	3.5.10). Withdrawn
1599		Incorporated into 03.05.07.

1600	5.5.11.	Authentication Feedback
1601		REQUIREMENT: 03.05.11
1602		ASSESSMENT OBJECTIVE
1603		Determine if:
1604 1605		A.03.05.11: feedback of authentication information during the authentication process is obscured.
1606		ASSESSMENT METHODS AND OBJECTS
1607		Examine
1608 1609 1610		[SELECT FROM: identification and authentication policy and procedures; procedures for authenticator feedback; system design documentation; system configuration settings; system audit records; system security plan; other relevant documents or records]
1611		Interview
1612 1613		[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]
1614		Test
1615 1616		[SELECT FROM: mechanisms for supporting and/or implementing the obscuring of feedback of authentication information during authentication]
1617		REFERENCES
1618		Source Assessment Procedure: <u>IA-06</u>
1619	3.5.12.	Authenticator Management
1620		REQUIREMENT: 03.05.12
1621		ACCECOMENT OF LECTIVE
1021		ASSESSMENT OBJECTIVE
1622		Determine if:
1622 1623		Determine if: A.03.05.12.ODP[01]: events that trigger the change or refreshment of authenticators are
1622 1623 1624 1625		Determine if: A.03.05.12.ODP[01]: events that trigger the change or refreshment of authenticators are defined. A.03.05.12.a: the identity of the individual, group, role, service, or device receiving the
1622 1623 1624 1625 1626 1627		 Determine if: A.03.05.12.ODP[01]: events that trigger the change or refreshment of authenticators are defined. A.03.05.12.a: the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution is verified. A.03.05.12.b: initial authenticator content for any authenticators issued by the organization is
1622 1623 1624 1625 1626 1627 1628 1629		A.03.05.12.ODP[01]: events that trigger the change or refreshment of authenticators are defined. A.03.05.12.a: the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution is verified. A.03.05.12.b: initial authenticator content for any authenticators issued by the organization is established. A.03.05.12.c[01]: administrative procedures for initial authenticator distribution are established
1622 1623 1624 1625 1626 1627 1628 1629 1630 1631		A.03.05.12.ODP[01]: events that trigger the change or refreshment of authenticators are defined. A.03.05.12.a: the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution is verified. A.03.05.12.b: initial authenticator content for any authenticators issued by the organization is established. A.03.05.12.c[01]: administrative procedures for initial authenticator distribution are established and implemented. A.03.05.12.c[02]: administrative procedures for lost, compromised, or damaged authenticators
1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633		A.03.05.12.ODP[01]: events that trigger the change or refreshment of authenticators are defined. A.03.05.12.a: the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution is verified. A.03.05.12.b: initial authenticator content for any authenticators issued by the organization is established. A.03.05.12.c[01]: administrative procedures for initial authenticator distribution are established and implemented. A.03.05.12.c[02]: administrative procedures for lost, compromised, or damaged authenticators are established and implemented. A.03.05.12.c[03]: administrative procedures for revoking authenticators are established and

1638	A.03.05.12.f[01]: authenticator content is protected from unauthorized disclosure.
1639	A.03.05.12.f[01]: authenticator content is protected from unauthorized modification.
1640	ASSESSMENT METHODS AND OBJECTS
1641	Examine
1642 1643 1644 1645	[SELECT FROM: identification and authentication policy and procedures; procedures for authenticator management; system configuration settings; list of system authenticator types; system design documentation; system audit records; change control records associated with managing system authenticators; system security plan; other relevant documents or records]
1646	Interview
1647 1648	[SELECT FROM: personnel with authenticator management responsibilities; personnel with information security responsibilities; system administrators]
1649	Test
1650 1651	[SELECT FROM: mechanisms for supporting and/or implementing the authenticator management capability]
1652	REFERENCES
1653	Source Assessment Procedure: <u>IA-05</u>
1654 1655	3.6. Incident Response 3.6.1. Incident Response Plan and Handling
1656	REQUIREMENT: 03.06.01
1657	ASSESSMENT OBJECTIVE
1658	Determine if:
1659 1660	A.03.06.01.a: an incident response plan that provides the organization with a roadmap for implementing its incident response capability is developed.
1661 1662	A.03.06.01.b[01]: an incident-handling capability for incidents that is consistent with the incident response plan is implemented.
1663	A.03.06.01.b[02]: the incident handling capability for incidents includes preparation.
1664	A.03.06.01.b[03]: the incident handling capability for incidents includes detection and analysis.
1665	A.03.06.01.b[04]: the incident handling capability for incidents includes containment.
1666	A.03.06.01.b[05]: the incident handling capability for incidents includes eradication.
1667	A.03.06.01.b[06]: the incident handling capability for incidents includes recovery.
1668 1669	A.03.06.01.c: the incident response plan is updated to address system and organizational changes or problems encountered during plan implementation, execution, or testing.
1670	ASSESSMENT METHODS AND OBJECTS
1671	Examine
1672 1673	[SELECT FROM: incident response policy and procedures; contingency planning policy and procedures; procedures for incident handling; procedures for incident response planning; incident

1674 1675		response plan; contingency plan; records of incident response plan reviews and approvals; system security plan; other relevant documents or records]
1676		Interview
1677 1678 1679		[SELECT FROM: personnel with incident handling responsibilities; personnel with incident response planning responsibilities; personnel with contingency planning responsibilities; personnel with information security responsibilities]
1680		Test
1681		[SELECT FROM: incident handling capability for the organization; incident response plan]
1682		REFERENCES
1683		Source Assessment Procedures: <u>IR-04</u> , <u>IR-08</u>
1684	3.6.2.	Incident Monitoring, Reporting, and Response Assistance
1685		REQUIREMENT: 03.06.02
1686		ASSESSMENT OBJECTIVE
1687		Determine if:
1688 1689		A.03.06.02.ODP[01]: the time period to report suspected incidents to the organizational incident response capability is defined.
1690		A.03.06.02.ODP[02]: authorities to whom incident information is to be reported are defined.
1691		A.03.06.02.a[01]: system security incidents are tracked.
1692		A.03.06.02.a[02]: system security incidents are documented.
1693 1694		A.03.06.02.b: suspected incidents are reported to the organizational incident response capability within < <i>A.03.06.02.ODP</i> [01]: time period>.
1695		A.03.06.02.c: incident information is reported to <a.03.06.02.odp[02]: authorities="">.</a.03.06.02.odp[02]:>
1696 1697		A.03.06.02.d: an incident response support resource that offers advice and assistance to users of the system for the handling and reporting of incidents is provided.
1698		ASSESSMENT METHODS AND OBJECTS
1699		Examine
1700 1701 1702		[SELECT FROM: incident response policy and procedures; procedures for incident monitoring; procedures for incident response assistance; incident response records and documentation; incident response plan; system security plan; other relevant documents or records]
1703		Interview
1704 1705 1706		[SELECT FROM: personnel with incident monitoring responsibilities; personnel with incident response assistance and support responsibilities; personnel with information security responsibilities]
1707		Test
1708 1709 1710 1711		[SELECT FROM: processes for incident reporting; incident monitoring capability; mechanisms for supporting and/or implementing the tracking and documenting of system security incidents; mechanisms for supporting and/or implementing incident reporting; mechanisms for supporting and/or implementing incident response assistance; processes for incident response assistance]

1712		REFERENCES
1713		Source Assessment Procedures: <u>IR-05</u> , <u>IR-06</u> , <u>IR-07</u>
1714	3.6.3.	Incident Response Testing
1715		REQUIREMENT: 03.06.03
1716		ASSESSMENT OBJECTIVE
1717		Determine if:
1718		A.03.06.03: the effectiveness of the incident response capability is tested periodically.
1719		ASSESSMENT METHODS AND OBJECTS
1720		Examine
1721 1722 1723 1724 1725		[SELECT FROM: incident response policy and procedures; contingency planning policy and procedures; procedures for incident response testing; procedures for contingency plan testing; incident response testing material; incident response test results; incident response test plan; incident response plan; contingency plan; system security plan; other relevant documents or records]
1726		Interview
1727 1728		[SELECT FROM: personnel with incident response testing responsibilities; personnel with information security responsibilities]
1729		REFERENCES
1730		Source Assessment Procedure: <u>IR-03</u>
1731	3.6.4.	Incident Response Training
1732		REQUIREMENT: 03.06.04
1733		ASSESSMENT OBJECTIVE
1734		Determine if:
1735 1736		A.03.06.04.ODP[01]: a time period within which incident response training is to be provided to system users is defined.
1737 1738		A.03.06.04.ODP[02]: events that initiate a review of the incident response training content are defined.
1739 1740 1741		A.03.06.04.a.01: incident response training for system users consistent with assigned roles and responsibilities is provided within <A.03.06.04.ODP[01]: time period > of assuming an incident response role or responsibility or acquiring system access.
1742 1743		A.03.06.04.a.02: incident response training for system users consistent with assigned roles and responsibilities is provided when required by system changes.
1744 1745		A.03.06.04.a.03: incident response training for system users consistent with assigned roles and responsibilities is provided periodically after initial and event-driven training.
1746		A.03.06.04.b[01]: incident response training content is reviewed periodically.
1747 1748		A.03.06.04.b[02]: incident response training content is reviewed following <a.03.06.04.odp[02]: events="">.</a.03.06.04.odp[02]:>

1749 A.03.06.04.b[03]: incident response training content is updated periodically. 1750 A.03.06.04.b[04]: incident response training content is updated following < A.03.06.04.ODP[02]: 1751 events>. 1752 ASSESSMENT METHODS AND OBJECTS 1753 **Examine** 1754 [SELECT FROM: incident response policy and procedures; procedures for incident response 1755 training; incident response training curriculum; incident response training materials; incident 1756 response plan; incident response training records; system security plan; other relevant 1757 documents or records1 1758 Interview 1759 [SELECT FROM: personnel with incident response training and operational responsibilities; 1760 personnel with information security responsibilities] 1761 **REFERENCES** 1762 Source Assessment Procedure: IR-02 1763 3.7. Maintenance 1764 **3.7.1.** Withdrawn 1765 Recategorized as NCO. 3.7.2. Withdrawn 1766 1767 Incorporated into 03.07.04 and 03.07.06. 1768 3.7.3. Withdrawn 1769 Incorporated into 03.08.03. 1770 3.7.4. Maintenance Tools 1771 REQUIREMENT: 03.07.04 1772 **ASSESSMENT OBJECTIVE** 1773 Determine if: 1774 **A.03.07.04.a[01]:** the use of system maintenance tools is approved. 1775 **A.03.07.04.a[02]:** the use of system maintenance tools is controlled. 1776 **A.03.07.04.a[03]:** the use of system maintenance tools is monitored. 1777 A.03.07.04.b: maintenance tools are inspected for improper or unauthorized modifications. 1778 A.03.07.04.c: media that contain diagnostic and test programs are checked for malicious code 1779 before being used in the system.

1780 A.03.07.04.d: the removal of system maintenance equipment containing CUI is prevented by 1781 verifying that there is no CUI on the equipment: sanitizing or destroying the equipment: or 1782 retaining the equipment within the facility. 1783 ASSESSMENT METHODS AND OBJECTS 1784 **Examine** 1785 [SELECT FROM: maintenance policy and procedures; procedures for system maintenance tools; 1786 system maintenance tools; maintenance tool inspection records; equipment sanitization records; 1787 media sanitization records; system security plan; other relevant documents or records] 1788 Interview 1789 [SELECT FROM: personnel with system maintenance responsibilities; personnel responsible for 1790 media sanitization; personnel with information security responsibilities] 1791 1792 [SELECT FROM: processes for approving, controlling, and monitoring maintenance tools; 1793 mechanisms for supporting and/or implementing the approval, control, and/or monitoring of 1794 maintenance tools; processes for preventing the unauthorized removal of information; processes 1795 for inspecting media for malicious code: mechanisms for supporting media sanitization or the 1796 destruction of equipment; mechanisms for supporting the verification of media sanitization; 1797 processes for inspecting maintenance tools; mechanisms for supporting and/or implementing the 1798 inspection of maintenance tools; mechanisms for supporting and/or implementing the inspection 1799 of media used for maintenance] 1800 **REFERENCES** 1801 Source Assessment Procedures: MA-03, MA-03(01), MA-03(02), MA-03(03) 1802 3.7.5. Nonlocal Maintenance 1803 REQUIREMENT: 03.07.05 1804 **ASSESSMENT OBJECTIVE** 1805 Determine if: 1806 A.03.07.05.a[01]: nonlocal maintenance and diagnostic activities are approved. 1807 A.03.07.05.a[02]: nonlocal maintenance and diagnostic activities are monitored. 1808 A.03.07.05.b: multi-factor authentication and replay resistance are implemented in the 1809 establishment of nonlocal maintenance and diagnostic sessions. 1810 A.03.07.05.c[01]: session connections are terminated when nonlocal maintenance is completed. 1811 A.03.07.05.c[02]: network connections are terminated when nonlocal maintenance is completed. 1812 ASSESSMENT METHODS AND OBJECTS 1813 **Examine** 1814 [SELECT FROM: maintenance policy and procedures; remote access policy and procedures; 1815 procedures for nonlocal system maintenance; records of remote access; maintenance records; 1816 diagnostic records; system design documentation; system configuration settings; system security 1817 plan; other relevant documents or records]

1818		Interview
1819 1820		[SELECT FROM: personnel with system maintenance responsibilities; personnel with information security responsibilities; system administrators]
1821		Test
1822 1823 1824 1825		[SELECT FROM: processes for managing nonlocal maintenance; mechanisms for implementing, supporting, and/or managing nonlocal maintenance; mechanisms for implementing multi-factor authentication and replay resistance; mechanisms for terminating nonlocal maintenance sessions and network connections]
1826		REFERENCES
1827		Source Assessment Procedure: MA-04
1828	3.7.6.	Maintenance Personnel
1829		REQUIREMENT: 03.07.06
1830		ASSESSMENT OBJECTIVE
1831		Determine if:
1832		A.03.07.06.a: a process for maintenance personnel authorization is established.
1833		A.03.07.06.b: a list of authorized maintenance organizations or personnel is maintained.
1834 1835		A.03.07.06.c: verification is performed that non-escorted personnel who perform maintenance on the system possess the required access authorizations.
1836 1837 1838		A.03.07.06.d: organizational personnel with required access authorizations and technical competence are designated to supervise the maintenance activities of personnel who do not possess the required access authorizations.
1839		ASSESSMENT METHODS AND OBJECTS
1840		Examine
1841 1842 1843		[SELECT FROM: maintenance policy and procedures; service provider contracts; service-level agreements; list of authorized personnel; maintenance records; access control records; system security plan; other relevant documents or records]
1844		Interview
1845 1846		[SELECT FROM: personnel with system maintenance responsibilities; personnel with information security responsibilities]
1847		Test
1848 1849		[SELECT FROM: processes for authorizing and managing maintenance personnel; mechanisms for supporting and/or implementing the authorization of maintenance personnel]
1850		REFERENCES
1851		Source Assessment Procedure: MA-05

1852	3.8.	<u>Media Protection</u>
1853	3.8.1.	Media Storage
1854		REQUIREMENT: 03.08.01
1855		ASSESSMENT OBJECTIVE
1856		Determine if:
1857 1858		A.03.08.01[01]: system media that contain CUI are physically controlled until the media are sanitized or destroyed using approved equipment, techniques, and procedures.
1859 1860		A.03.08.01[02]: system media that contain CUI are securely stored until the media are sanitized or destroyed using approved equipment, techniques, and procedures.
1861		ASSESSMENT METHODS AND OBJECTS
1862		Examine
1863 1864 1865		[SELECT FROM: physical protection policy and procedures; media protection policy and procedures; procedures for media storage; access control policy and procedures; system media; system security plan; other relevant documents or records]
1866		Interview
1867 1868		[SELECT FROM: personnel with system media protection and storage responsibilities; personnel with information security responsibilities]
1869		Test
1870 1871		[SELECT FROM: processes for storing information media; mechanisms for supporting and/or implementing secure media storage/media protection]
1872		REFERENCES
1873		Source Assessment Procedure: MP-04
1874	3.8.2.	Media Access
1875		REQUIREMENT: 03.08.02
1876		ASSESSMENT OBJECTIVE
1877		Determine if:
1878		A.03.08.02: access to CUI on system media is restricted.
1879		ASSESSMENT METHODS AND OBJECTS
1880		Examine
1881 1882 1883 1884		[SELECT FROM: physical protection policy and procedures; media protection policy and procedures; procedures for media access restrictions; access control policy and procedures; media storage facilities; access control records; system security plan; other relevant documents or records]
1885		Interview
1886 1887		[SELECT FROM: personnel with system media protection responsibilities; personnel with information security responsibilities; system administrators]

1888 Test 1889 [SELECT FROM: processes for restricting information on media; mechanisms supporting and/or 1890 implementing media access restrictions] 1891 REFERENCES 1892 Source Assessment Procedure: MP-02 1893 3.8.3. Media Sanitization 1894 **REQUIREMENT: 03.08.03** 1895 **ASSESSMENT OBJECTIVE** 1896 Determine if: 1897 A.03.08.03: system media that contain CUI are sanitized prior to disposal, release out of 1898 organizational control, or release for reuse. 1899 ASSESSMENT METHODS AND OBJECTS 1900 Examine 1901 [SELECT FROM: media protection policy and procedures; procedures for media sanitization and 1902 disposal; applicable standards and policies that address media sanitization policy; system audit 1903 records; media sanitization records; system design documentation; system configuration settings; 1904 records retention and disposition policy; records retention and disposition procedures; system 1905 security plan; other relevant documents or records] 1906 Interview 1907 [SELECT FROM: personnel with media sanitization responsibilities; personnel with records 1908 retention and disposition responsibilities; personnel with information security responsibilities; 1909 system administrators] 1910 Test 1911 [SELECT FROM: processes for media sanitization; mechanisms for supporting and/or 1912 implementing media sanitization] 1913 REFERENCES 1914 Source Assessment Procedure: MP-06 1915 3.8.4. Media Marking 1916 REQUIREMENT: 03.08.04 1917 **ASSESSMENT OBJECTIVE** 1918 Determine if: 1919 A.03.08.04[01]: system media that contain CUI are marked to indicate distribution limitations. 1920 A.03.08.04[02]: system media that contain CUI are marked to indicate handling caveats. 1921 A.03.08.04[03]: system media that contain CUI are marked to indicate security markings.

1922 ASSESSMENT METHODS AND OBJECTS 1923 **Examine** 1924 [SELECT FROM: physical protection policy and procedures: media protection policy and 1925 procedures; procedures for media marking; list of system media marking security attributes; 1926 system security plan; other relevant documents or records] 1927 Interview 1928 [SELECT FROM: personnel with system media protection and marking responsibilities; personnel 1929 with information security responsibilities1 1930 Test 1931 [SELECT FROM: processes for marking information media; mechanisms for supporting and/or 1932 implementing media marking] 1933 REFERENCES 1934 Source Assessment Procedure: MP-03 1935 3.8.5. Media Transport 1936 **REQUIREMENT: 03.08.05** 1937 **ASSESSMENT OBJECTIVE** 1938 Determine if: 1939 A.03.08.05.a[01]: system media that contain CUI are protected during transport outside of 1940 controlled areas. 1941 A.03.08.05.a[02]: system media that contain CUI are controlled during transport outside of 1942 controlled areas. 1943 A.03.08.05.b: the accountability of system media that contain CUI is maintained during transport 1944 outside of controlled areas. 1945 A.03.08.05.c: cryptographic mechanisms are implemented to prevent the unauthorized disclosure 1946 of CUI stored on digital media during transport. 1947 ASSESSMENT METHODS AND OBJECTS 1948 **Examine** 1949 [SELECT FROM: physical protection policy and procedures; media protection policy and 1950 procedures; procedures for media storage; access control policy and procedures; authorized 1951 personnel list: system media: designated controlled areas: system and communications 1952 protection policy and procedures; cryptographic mechanisms and configuration documentation; 1953 procedures for the protection of information at rest; system design documentation; system 1954 configuration settings: list of information at rest requiring confidentiality protections; system audit 1955 records; system security plan; other relevant documents or records] 1956 Interview 1957 [SELECT FROM: personnel with system media protection and storage responsibilities; personnel 1958 with information security responsibilities; system developers; system administrators]

Incorporated into <u>03.08.07</u>.

1990

1959		Test
1960 1961 1962		[SELECT FROM: processes for storing information media; mechanisms for supporting and/or implementing media storage/media protection; mechanisms for supporting and/or implementing confidentiality protections for information at rest]
1963		REFERENCES
1964		Source Assessment Procedures: MP-05, SC-28, SC-28(01)
1965	3.8.6.	Withdrawn
1966		Incorporated into <u>03.08.05</u> .
1967	3.8.7.	Media Use
1968		REQUIREMENT: 03.08.07
1969		ASSESSMENT OBJECTIVE
1970		Determine if:
1971 1972		A.03.08.07.ODP[01]: the types of system media with usage restrictions or that are prohibited from use are defined.
1973 1974		A.03.08.07.a: the use of the following types of system media is restricted or prohibited: < A.03.08.07.ODP[01]: types of system media>.
1975		A.03.08.07.b: the use of removable system media without an identifiable owner is prohibited.
1976		ASSESSMENT METHODS AND OBJECTS
1977		Examine
1978 1979 1980		[SELECT FROM: system media protection policy and procedures; system use policy; procedures for media usage restrictions; rules of behavior; system design documentation; audit records; system configuration settings; system security plan; other relevant documents or records]
1981		Interview
1982 1983		[SELECT FROM: personnel with system media use responsibilities; personnel with information security responsibilities; system administrators]
1984		Test
1985 1986		[SELECT FROM: processes for media use; mechanisms for restricting or prohibiting the use of system media on systems or system components]
1987		REFERENCES
1988		Source Assessment Procedure: MP-07
1989	3.8.8.	Withdrawn

1991	3.8.9.	System Backup – Cryptographic Protection
1992		REQUIREMENT: 03.08.09
1993		ASSESSMENT OBJECTIVE
1994		Determine if:
1995 1996		A.03.08.09: cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI at backup storage locations.
1997		ASSESSMENT METHODS AND OBJECTS
1998		Examine
1999 2000 2001		[SELECT FROM: contingency planning policy and procedures; procedures for system backup; contingency plan; system design documentation; system configuration settings; system security plan; other relevant documents or records]
2002		Interview
2003 2004		[SELECT FROM: personnel with system backup responsibilities; personnel with information security responsibilities]
2005		Test
2006 2007		[SELECT FROM: mechanisms for supporting and/or implementing the cryptographic protection of backup information]
2008		REFERENCES
2009		Source Assessment Procedure: <u>CP-09(08)</u>
2010	3.9.	Personnel Security
2011	3.9.1.	Personnel Screening
2012		REQUIREMENT: 03.09.01
2013		ASSESSMENT OBJECTIVE
2014		Determine if:
2015		A.03.09.01.ODP[01]: the conditions that require the rescreening of individuals are defined.
2016		A.03.09.01.a: individuals are screened prior to authorizing access to the system.
2017 2018		A.03.09.01.b: individuals are rescreened in accordance with the following conditions: < <i>A.03.09.01.ODP[01]: conditions></i> .
2019		ASSESSMENT METHODS AND OBJECTS
2020		Examine
2021 2022		[SELECT FROM: personnel security policy and procedures; procedures for personnel screening; records of screened personnel; system security plan; other relevant documents or records]
2023		Interview
2024 2025		[SELECT FROM: personnel with personnel security responsibilities; personnel with information security responsibilities]

administrators]

2026 Test 2027 ISELECT FROM: processes for personnel screening. 2028 REFERENCES 2029 Source Assessment Procedure: PS-03 3.9.2. Personnel Termination and Transfer 2030 2031 **REQUIREMENT: 03.09.02** 2032 ASSESSMENT OBJECTIVE 2033 Determine if: 2034 A.03.09.02.ODP[01]: the time period within which to disable system access is defined. 2035 A.03.09.02.ODP[02]: the time period within which transfer or reassignment actions must 2036 occur following an individual transfer or reassignment is defined. 2037 A.03.09.02.ODP[03]: the transfer or reassignment actions to be initiated following transfer 2038 or reassignment are defined. 2039 A.03.09.02.a.01: upon the termination of individual employment, system access is disabled within 2040 <A.03.09.02.ODP[01]: time period>. 2041 A.03.09.02.a.02: upon the termination of individual employment, authenticators and credentials 2042 associated with the individual are terminated or revoked. 2043 A.03.09.02.a.03: upon the termination of individual employment, security-related system property 2044 is retrieved. 2045 A.03.09.02.b.01: upon individual reassignment or transfer to other positions in the organization, 2046 the ongoing operational need for current logical and physical access authorizations to the system 2047 and facility are reviewed and confirmed. 2048 A.03.09.02.b.02: upon individual reassignment or transfer to other positions in the organization, 2049 the following transfer or reassignment actions are initiated within < A.03.09.02.ODP[02]: time period>: <A.03.09.02.ODP[03]: transfer or reassignment actions>. 2050 2051 A.03.09.02.b.03: upon individual reassignment or transfer to other positions in the organization. 2052 access authorization is modified to correspond with any changes in operational need. 2053 ASSESSMENT METHODS AND OBJECTS 2054 **Examine** 2055 [SELECT FROM: personnel security policy and procedures; procedures for personnel 2056 termination; records of personnel transfer actions; procedures for personnel transfer; list of 2057 system and facility access authorizations; records of personnel termination actions; records of 2058 terminated or revoked authenticators or credentials; list of system accounts; records of exit 2059 interviews; system security plan; other relevant documents or records] 2060 Interview 2061 [SELECT FROM: personnel with personnel security responsibilities; personnel with account 2062 management responsibilities; personnel with information security responsibilities; system 2063

2064	Test
2065 2066 2067 2068	[SELECT FROM: processes for personnel termination; processes for personnel transfer; mechanisms for supporting and/or implementing personnel transfer notifications; mechanisms for supporting and/or implementing personnel termination notifications; mechanisms for disabling system access and revoking authenticators]
2069	REFERENCES
2070	Source Assessment Procedures: <u>PS-04</u> , <u>PS-05</u>
2071	3.10. Physical Protection
2072	3.10.1. Physical Access Authorizations
2073	REQUIREMENT: 03.10.01
2074	ASSESSMENT OBJECTIVE
2075	Determine if:
2076 2077	A.03.10.01.a[01]: a list of individuals with authorized access to the physical location where the system resides is developed.
2078 2079	A.03.10.01.a[02]: a list of individuals with authorized access to the physical location where the system resides is approved.
2080 2081	A.03.10.01.a[03]: a list of individuals with authorized access to the physical location where the system resides is maintained.
2082	A.03.10.01.b: authorization credentials are issued for facility access.
2083	A.03.10.01.c: the physical access list is reviewed periodically.
2084 2085	A.03.10.01.d: individuals from the physical access list are removed when access is no longer required.
2086	ASSESSMENT METHODS AND OBJECTS
2087	Examine
2088 2089 2090 2091	[SELECT FROM: physical protection policy and procedures; procedures for physical access authorizations; authorized personnel access list; physical access list reviews; physical access termination records; authorization credentials; system security plan; other relevant documents or records]
2092	Interview
2093 2094 2095	[SELECT FROM: personnel with physical access authorization responsibilities; personnel with physical access to the facility where the system resides; personnel with information security responsibilities]
2096	Test
2097 2098	[SELECT FROM: processes for physical access authorizations; mechanisms for supporting and/or implementing physical access authorizations]
2099	REFERENCES
2100	Source Assessment Procedure: <u>PE-02</u>

2101	3.10.2.	Monitoring Physical Access
2102		REQUIREMENT: 03.10.02
2103		ASSESSMENT OBJECTIVE
2104		Determine if:
2105 2106		A.03.10.02.a[01]: physical access to the location where the system resides is monitored to detect physical security incidents.
2107 2108		A.03.10.02.a[02]: physical access to the location where the system resides is monitored to respond to physical security incidents.
2109		A.03.10.02.b: physical access logs are reviewed periodically.
2110		ASSESSMENT METHODS AND OBJECTS
2111		Examine
2112 2113 2114		[SELECT FROM: physical protection policy and procedures; procedures for physical access monitoring; physical access logs or records; physical access monitoring records; physical access log reviews; system security plan; other relevant documents or records]
2115		Interview
2116 2117		[SELECT FROM: personnel with physical access monitoring responsibilities; personnel with incident response responsibilities; personnel with information security responsibilities]
2118		Test
2119 2120 2121		[SELECT FROM: processes for monitoring physical access; mechanisms supporting and/or implementing physical access monitoring; mechanisms supporting and/or implementing the review of physical access logs]
2122		REFERENCES
2123		Source Assessment Procedure: <u>PE-06</u>
2124	3.10.3.	Withdrawn
2125		Incorporated into <u>03.10.07</u> .
2126	3.10.4.	Withdrawn
2127		Incorporated into <u>03.10.07</u> .
2128	3.10.5.	Withdrawn
2129		Incorporated into <u>03.10.07</u> .
2130	3.10.6.	Alternate Work Site
2131		REQUIREMENT: 03.10.06
2132		ASSESSMENT OBJECTIVE
2133		Determine if:

2134 2135		A.03.10.06.ODP[01]: the security requirements to be employed at alternate work sites are defined.
2136		A.03.10.06.a: alternate work sites allowed for use by employees are defined.
2137 2138		A.03.10.06.b: the following security requirements are employed at alternate work sites: < A.03.10.06.ODP[01]: security requirements>.
2139		ASSESSMENT METHODS AND OBJECTS
2140		Examine
2141 2142 2143		[SELECT FROM: physical protection policy and procedures; procedures for alternate work sites for personnel; list of security requirements for alternate work sites; assessments of security requirements at alternate work sites; system security plan; other relevant documents or records]
2144		Interview
2145 2146 2147		[SELECT FROM: personnel approving the use of alternate work sites; personnel using alternate work sites; personnel assessing security requirements at alternate work sites; personnel with information security responsibilities]
2148		Test
2149 2150 2151		[SELECT FROM: processes for security at alternate work sites; mechanisms for supporting alternate work sites; security requirements employed at alternate work sites; means of communication between personnel at alternate work sites and security personnel]
2152		REFERENCES
2153		Source Assessment Procedure: <u>PE-17</u>
2154	3.10.7.	Physical Access Control
2155		REQUIREMENT: 03.10.07
2156		ASSESSMENT OBJECTIVE
2157		Determine if:
2158 2159		A.03.10.07.ODP[01]: the circumstances requiring visitor escorts and control of visitor activity are defined.
2160 2161		A.03.10.07.a.01: physical access is controlled at the location where the system resides by verifying individual physical access authorizations before granting access.
2162 2163		A.03.10.07.a.02: physical access is controlled at the location where the system resides by controlling ingress and egress with physical access control systems/devices or guards.
2164		A.03.10.07.b: physical access audit logs for entry or exit points are maintained.
2165		A.03.10.07.c[01]: visitors are escorted.
2166 2167		A.03.10.07.c[02]: visitor activity is controlled under the following circumstances: <a.03.10.07.odp[01]: circumstances="">.</a.03.10.07.odp[01]:>
2168		A.03.10.07.d[01]: keys are secured.
2169		A.03.10.07.d[02]: combinations are secured.
2170		A.03.10.07.d[03]: other physical access devices are secured.

2171 ASSESSMENT METHODS AND OBJECTS 2172 **Examine** 2173 ISELECT FROM: physical protection policy and procedures: procedures for physical access 2174 control; physical access control logs or records; inventory records of physical access control 2175 devices; system entry and exit points; records of key and lock combination changes; storage 2176 locations for physical access control devices; physical access control devices; list of security 2177 safeguards controlling access to designated publicly accessible areas within facility; system 2178 security plan; other relevant documents or records] 2179 Interview 2180 [SELECT FROM: personnel with physical access control responsibilities; personnel with 2181 information security responsibilities] 2182 Test 2183 [SELECT FROM: processes for physical access control; mechanisms for supporting and/or 2184 implementing physical access control; physical access control devices] 2185 **REFERENCES** 2186 Source Assessment Procedure: PE-03 2187 3.10.8. Access Control for Transmission and Output Devices 2188 **REQUIREMENT: 03.10.08** 2189 **ASSESSMENT OBJECTIVE** 2190 Determine if: 2191 A.03.10.08.a: physical access to system distribution and transmission lines in organizational 2192 facilities is controlled. 2193 A.03.10.08.b: physical access to output devices is controlled to prevent unauthorized 2194 individuals from obtaining access to CUI. 2195 ASSESSMENT METHODS AND OBJECTS 2196 **Examine** 2197 [SELECT FROM: physical protection policy and procedures; procedures for access control for 2198 transmission mediums; system design documentation; facility communications and wiring 2199 diagrams; list of physical security safeguards applied to system distribution and transmission 2200 lines; procedures for access control for display medium; facility layout of system components; 2201 actual displays from system components; list of output devices and associated outputs that 2202 require physical access controls; physical access control logs or records for areas containing 2203 output devices and related outputs; system security plan; other relevant documents or records] 2204 Interview 2205 [SELECT FROM: personnel with physical access control responsibilities; personnel with 2206 information security responsibilities] 2207 **Test** 2208 [SELECT FROM: processes for access control for distribution and transmission lines; 2209 mechanisms for supporting and/or implementing access control for distribution and transmission 2210 lines; processes for access control to output devices; mechanisms for supporting and/or 2211 implementing access control for output devices]

2212		REFERENCES
2213		Source Assessment Procedures: <u>PE-04</u> , <u>PE-05</u>
2214	3.11.	Risk Assessment
2215	3.11.1	. Risk Assessment
2216		REQUIREMENT: 03.11.01
2217		ASSESSMENT OBJECTIVE
2218		Determine if:
2219 2220		A.03.11.01.a: the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.
2221		A.03.11.01.b: risk assessments are updated periodically.
2222		ASSESSMENT METHODS AND OBJECTS
2223		Examine
2224 2225 2226 2227 2228 2229		[SELECT FROM: risk assessment policy and procedures; security planning policy and procedures; procedures for organizational assessments of risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; SCRM policy and procedures; inventory of critical systems, system components, and system services; procedures for organizational assessments of supply chain risk; acquisition policy; SCRM plan; system security plan; other relevant documents or records]
2230		Interview
2231 2232		[SELECT FROM: personnel with risk assessment responsibilities; personnel with SCRM responsibilities; personnel with security responsibilities]
2233		Test
2234 2235 2236 2237		[SELECT FROM: processes for organizational risk assessments; mechanisms for supporting and/or conducting, documenting, reviewing, disseminating, and updating risk assessments; mechanisms supporting and/or conducting, documenting, reviewing, disseminating, and updating supply chain risk assessments]
2238		REFERENCES
2239		Source Assessment Procedures: <u>RA-03</u> , <u>RA-03(01)</u> , <u>SR-06</u>
2240	3.11.2	. Vulnerability Monitoring and Scanning
2241		REQUIREMENT: 03.11.02
2242		ASSESSMENT OBJECTIVE
2243		Determine if:
2244		A.03.11.02.ODP[01]: response times to remediate system vulnerabilities are defined.
2245		A.03.11.02.a[01]: the system is monitored for vulnerabilities periodically.
2246 2247		A.03.11.02.a[02]: the system is monitored for vulnerabilities when new vulnerabilities that affect the system are identified.

2248	A.03.11.02.a[03]: the system is scanned for vulnerabilities periodically.	
2249 2250	A.03.11.02.a[04]: the system is scanned for vulnerabilities when new vulnerabilities that affective system are identified.	эct
2251	A.03.11.02.b: system vulnerabilities are remediated < A.03.11.02.ODP[01]: response times	s>.
2252	A.03.11.02.c[01]: system vulnerabilities to be scanned are updated periodically.	
2253 2254	A.03.11.02.c[02]: system vulnerabilities to be scanned are updated when new vulnerabilitie are identified.	s
2255 2256	A.03.11.02.c[03]: system vulnerabilities to be scanned are updated when new vulnerabilitie are reported.	S
2257	ASSESSMENT METHODS AND OBJECTS	
2258	Examine	
2259 2260 2261 2262	[SELECT FROM: risk assessment policy and procedures; procedures for vulnerability scann patch and vulnerability management records; vulnerability scanning tools and configuration documentation; vulnerability scanning results; risk assessment; risk assessment report; system security plan; other relevant documents or records]	•
2263	Interview	
2264 2265 2266 2267	[SELECT FROM: personnel with risk assessment and vulnerability scanning responsibilities personnel with vulnerability scan analysis responsibilities; personnel with vulnerability remediation responsibilities; personnel with information security responsibilities; system administrators]	ţ
2268	Test	
2269 2270	[SELECT FROM: processes for vulnerability scanning, analysis, and remediation; mechanis for supporting and/or implementing vulnerability scanning, analysis, and remediation]	ms
2271	REFERENCES	
2272	Source Assessment Procedures: <u>RA-05</u> , <u>RA-05(02)</u>	
2273	3.11.3. Withdrawn	
2274	Incorporated into <u>03.11.02</u> .	
2275	3.12. Security Assessment and Monitoring	
2276	3.12.1. Security Assessment	
2277	REQUIREMENT: 03.12.01	
2278	ASSESSMENT OBJECTIVE	
2279	Determine if:	
2280 2281	A.03.12.01: the security requirements for the system and its environment of operation are assessed periodically to determine if the requirements have been satisfied.	

2282		ASSESSMENT METHODS AND OBJECTS
2283		Examine
2284 2285 2286		[SELECT FROM: security assessment and monitoring policy and procedures; procedures for security assessment planning; security assessment plan; security assessment report; system security plan; other relevant documents or records]
2287		Interview
2288 2289		[SELECT FROM: personnel with security assessment responsibilities; personnel with information security responsibilities]
2290		Test
2291 2292		[SELECT FROM: mechanisms supporting security assessments, processes for security assessment plan development and/or security assessment reporting]
2293		REFERENCES
2294		Source Assessment Procedure: <u>CA-02</u>
2295	3.12.2.	Plan of Action and Milestones
2296		REQUIREMENT: 03.12.02
2297		ASSESSMENT OBJECTIVE
2298		Determine if:
2299 2300 2301		A.03.12.02.a.01: a plan of action and milestones for the system is developed to document the planned remediation actions for correcting weaknesses or deficiencies noted during security assessments.
2302 2303		A.03.12.02.a.02: a plan of action and milestones for the system is developed to reduce or eliminate known system vulnerabilities.
2304 2305		A.03.12.02.b[01]: the existing plan of action and milestones is updated periodically based on the findings from security assessments.
2306 2307		A.03.12.02.b[02]: the existing plan of action and milestones is updated periodically based on the findings from independent audits or reviews.
2308 2309		A.03.12.02.b[03]: the existing plan of action and milestones is updated periodically based on the findings from continuous monitoring activities.
2310		ASSESSMENT METHODS AND OBJECTS
2311		Examine
2312 2313 2314 2315		[SELECT FROM: security assessment and monitoring policy and procedures; procedures for plans of action and milestones; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; system security plan; other relevant documents or records]
2316		Interview
2317 2318		[SELECT FROM: personnel with plans of action and milestones development and implementation responsibilities; personnel with information security responsibilities]
2319		Test
2320 2321		[SELECT FROM: mechanisms for developing, implementing, and maintaining plans of action and milestones]

November 2	023
------------	-----

2322		REFERENCES
2323		Source Assessment Procedure: <u>CA-05</u>
2324	3.12.3.	Continuous Monitoring
2325		REQUIREMENT: 03.12.03
2326		ASSESSMENT OBJECTIVE
2327		Determine if:
2328		A.03.12.03[01]: a system-level continuous monitoring strategy is developed and implemented.
2329		A.03.12.03[02]: ongoing monitoring is included in the continuous monitoring strategy.
2330		A.03.12.03[03]: security assessments are included the continuous monitoring strategy.
2331		ASSESSMENT METHODS AND OBJECTS
2332		Examine
2333 2334 2335 2336 2337 2338		[SELECT FROM: security assessment and monitoring policy and procedures; organizational continuous monitoring strategy; system-level continuous monitoring strategy; procedures for continuous monitoring of the system; procedures for configuration management; security assessment report; plan of action and milestones; system monitoring records; configuration management records; impact analyses; status reports; system security plan; other relevant documents or records]
2339		Interview
2340 2341		[SELECT FROM: personnel with continuous monitoring responsibilities; personnel with information security responsibilities; system administrators]
2342		Test
2343 2344 2345		[SELECT FROM: mechanisms for implementing continuous monitoring; mechanisms supporting response actions for assessment and monitoring results; mechanisms for supporting security status reporting]
2346		REFERENCES
2347		Source Assessment Procedure: <u>CA-07</u>
2348	3.12.4.	Withdrawn
2349		Incorporated into <u>03.15.02</u> .
2350	2 12 5	Information Exchange
	3.12.3.	•
2351		REQUIREMENT: 03.12.05
2352		ASSESSMENT OBJECTIVE
2353		Determine if:
2354 2355		A.03.12.05.ODP[01]: one or more of the following parameter values is/are selected: {interconnection security agreements; information exchange security agreements;

2356 2357	memoranda of understanding or agreement; service-level agreements; user agreements non-disclosure agreements}.
2358 2359	A.03.12.05.a: the exchange of CUI between the system and other systems is approved and managed using <A.03.12.05.ODP[01]: selected parameter value(s)>.
2360 2361	A.03.12.05.b[01]: interface characteristics are documented as part of the exchange agreements.
2362	A.03.12.05.b[02]: security requirements are documented as part of the exchange agreements.
2363 2364	A.03.12.05.b[03]: responsibilities for each system are documented as part of the exchange agreements.
2365	A.03.12.05.c[01]: exchange agreements are reviewed periodically.
2366	A.03.12.05.c[02]: exchange agreements are updated periodically.
2367	ASSESSMENT METHODS AND OBJECTS
2368	Examine
2369 2370 2371 2372 2373 2374	[SELECT FROM: access control policy and procedures; procedures for system connections; system and communications protection policy and procedures; system interconnection security agreements; information exchange security agreements; service-level agreements; memoranda of understanding or agreements; non-disclosure agreements; system design documentation; enterprise architecture; security architecture; system configuration settings; system security plan; other relevant documents or records]
2375	Interview
2376 2377 2378	[SELECT FROM: personnel with development, implementation, and approval responsibilities for system interconnection agreements; personnel who manage systems to which the exchange agreements apply; personnel with information security responsibilities]
2379	REFERENCES
2380	Source Assessment Procedure: <u>CA-03</u>
2381	3.13. System and Communications Protection
2382	3.13.1. Boundary Protection
2383	REQUIREMENT: 03.13.01
2384	ASSESSMENT OBJECTIVE
2385	Determine if:
2386	A.03.13.01.a[01]: communications at external managed interfaces to the system are monitored
2387	A.03.13.01.a[02]: communications at external managed interfaces to the system are controlled
2388 2389	A.03.13.01.a[03]: communications at key internal managed interfaces within the system are monitored.
2390 2391	A.03.13.01.a[04]: communications at key internal managed interfaces within the system are controlled.
2392 2393	A.03.13.01.b: subnetworks are implemented for publicly accessible system components that are physically or logically separated from internal networks.

2394 A.03.13.01.c: external system connections are only made through managed interfaces that 2395 consist of boundary protection devices arranged in accordance with an organizational security 2396 architecture. 2397 ASSESSMENT METHODS AND OBJECTS 2398 **Examine** 2399 [SELECT FROM: system and communications protection policy and procedures; procedures for 2400 boundary protection; list of key internal boundaries within the system; boundary protection 2401 hardware and software; system configuration settings; security architecture; system audit 2402 records: system design documentation: system security plan; other relevant documents or 2403 records1 2404 Interview 2405 [SELECT FROM: personnel with boundary protection responsibilities; personnel with 2406 information security responsibilities; system developers; system administrators] 2407 2408 ISELECT FROM: mechanisms for implementing boundary protection capabilities 2409 **REFERENCES** 2410 Source Assessment Procedure: SC-07 3.13.2. Withdrawn 2411 2412 Recategorized as NCO. 3.13.3. Withdrawn 2413 2414 Addressed by 03.01.04, 03.01.05, 03.01.06, and 03.01.07. 3.13.4. Information in Shared System Resources 2415 2416 **REQUIREMENT: 03.13.04** 2417 ASSESSMENT OBJECTIVE 2418 Determine if: 2419 A.03.13.04[01]: unauthorized information transfer via shared system resources is prevented. 2420 A.03.13.04[02]: unintended information transfer via shared system resources is prevented. 2421 **ASSESSMENT METHODS AND OBJECTS** 2422 **Examine** 2423 [SELECT FROM: system and communications protection policy and procedures; procedures for 2424 information protection in shared system resources; system configuration settings; system audit 2425 records; system design documentation; system security plan; other relevant documents or 2426 records]

2458

REQUIREMENT: 03.13.08

2427		Interview
2428 2429		[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]
2430		Test
2431 2432		[SELECT FROM: mechanisms for preventing the unauthorized and unintended transfer of information via shared system resources]
2433		REFERENCES
2434		Source Assessment Procedure: <u>SC-04</u>
2435	3.13.5.	Withdrawn
2436		Incorporated into <u>03.13.01</u> .
2437	3.13.6.	Network Communications – Deny by Default – Allow by Exception
2438		REQUIREMENT: 03.13.06
2439		ASSESSMENT OBJECTIVE
2440		Determine if:
2441		A.03.13.06[01]: network communications traffic is denied by default.
2442		A.03.13.06[02]: network communications traffic is allowed by exception.
2443		ASSESSMENT METHODS AND OBJECTS
2444		Examine
2445 2446 2447		[SELECT FROM: system and communications protection policy and procedures; procedures fo boundary protection; system design documentation; system configuration settings; system audi records; system security plan; other relevant documents or records]
2448		Interview
2449 2450		[SELECT FROM: personnel with boundary protection responsibilities; personnel with information security responsibilities; system developers; system administrators]
2451		Test
2452		[SELECT FROM: mechanisms for implementing traffic management at managed interfaces]
2453		REFERENCES
2454		Source Assessment Procedure: <u>SC-07(05)</u>
2455	3.13.7.	Withdrawn
2456		Addressed by <u>03.01.12</u> , <u>03.04.02</u> and <u>03.04.06</u> .
2457	3.13.8.	Transmission and Storage Confidentiality

2459 **ASSESSMENT OBJECTIVE** 2460 Determine if: 2461 A.03.13.08[01]: cryptographic mechanisms are implemented to prevent the unauthorized 2462 disclosure of CUI during transmission. 2463 A.03.13.08[02]: cryptographic mechanisms are implemented to prevent the unauthorized 2464 disclosure of CUI while in storage. 2465 ASSESSMENT METHODS AND OBJECTS 2466 **Examine** 2467 [SELECT FROM: system and communications protection policy and procedures; procedures for 2468 transmission confidentiality; procedures for the protection of information at rest; system design 2469 documentation; system configuration settings; cryptographic mechanisms and associated 2470 configuration documentation; information in storage requiring confidentiality protection; system 2471 audit records; system security plan; other relevant documents or records] 2472 Interview 2473 [SELECT FROM: personnel with information security responsibilities; system developers; 2474 system administrators] 2475 **Test** 2476 [SELECT FROM: mechanisms for supporting and/or implementing transmission confidentiality; 2477 cryptographic mechanisms for supporting and/or implementing transmission confidentiality; 2478 mechanisms for supporting and/or implementing confidentiality protection for information in 2479 storage; cryptographic mechanisms implementing confidentiality protections for information in 2480 storage] 2481 **REFERENCES** 2482 Source Assessment Procedures: SC-08, SC-08(01), SC-28, SC-28(01) 2483 3.13.9. Network Disconnect 2484 **REQUIREMENT: 03.13.09** 2485 **ASSESSMENT OBJECTIVE** 2486 Determine if: 2487 A.03.13.09: network connections associated with communications sessions are terminated at 2488 the end of the sessions or after periods of inactivity. 2489 ASSESSMENT METHODS AND OBJECTS 2490 **Examine** 2491 [SELECT FROM: system and communications protection policy and procedures; procedures for 2492 network disconnect; system design documentation; system configuration settings; system audit 2493 records; system security plan; other relevant documents or records] 2494 Interview 2495 [SELECT FROM: personnel with information security responsibilities; system developers; 2496 system administrators]

2531 2532

	November	2023
2497		Test
2498 2499		[SELECT FROM: mechanisms for supporting and/or implementing a network disconnect capability]
2500		REFERENCES
2501		Source Assessment Procedure: <u>SC-10</u>
2502	3.13.10.	Cryptographic Key Establishment and Management
2503		REQUIREMENT: 03.13.10
2504		ASSESSMENT OBJECTIVE
2505		Determine if:
2506		A.03.13.10.ODP[01]: requirements for key establishment and management are defined.
2507 2508		A.03.13.10[01]: cryptographic keys are established in the system in accordance with the following key management requirements: < A.03.13.10.ODP[01]: requirements> .
2509 2510		A.03.13.10[02]: cryptographic keys are managed in the system in accordance with the following key management requirements: < <i>A.03.13.10.ODP[01]:</i> requirements>.
2511		ASSESSMENT METHODS AND OBJECTS
2512		Examine
2513 2514 2515 2516		[SELECT FROM: system and communications protection policy and procedures; procedures for cryptographic key establishment and management; system design documentation; system configuration settings; cryptographic mechanisms; system audit records; system security plan other relevant documents or records]
2517		Interview
2518 2519		[SELECT FROM: personnel with responsibilities for cryptographic key establishment and/or management; personnel with information security responsibilities; system administrators]
2520		Test
2521 2522		[SELECT FROM: mechanisms for supporting and/or implementing cryptographic key establishment and management]
2523		REFERENCES
2524		Source Assessment Procedure: <u>SC-12</u>
2525	3.13.11.	Cryptographic Protection
2526		REQUIREMENT: 03.13.11
2527		ASSESSMENT OBJECTIVE
2528		Determine if:
2529 2530		A.03.13.11.ODP[01]: the types of cryptography for protecting the confidentiality of CUI are defined.

A.03.13.11: the following types of cryptography are implemented when used to protect the confidentiality of CUI: <**A.03.13.11.ODP[01]:** types of cryptography>.

2533		ASSESSMENT METHODS AND OBJECTS
2534		Examine
2535 2536 2537 2538		[SELECT FROM: system and communications protection policy and procedures; procedures for cryptographic protection; system design documentation; system configuration settings; cryptographic module validation certificates; list of FIPS-validated cryptographic modules; system audit records; system security plan; other relevant documents or records]
2539		Interview
2540 2541		[SELECT FROM: personnel with responsibilities for cryptographic protection; personnel with information security responsibilities; system developers; system administrators]
2542		Test
2543		[SELECT FROM: mechanisms for supporting and/or implementing cryptographic protection]
2544		REFERENCES
2545		Source Assessment Procedure: <u>SC-13</u>
2546	3.13.12.	Collaborative Computing Devices and Applications
2547		REQUIREMENT: 03.13.12
2548		ASSESSMENT OBJECTIVE
2549		Determine if:
2550 2551		A.03.13.12.a: remote activation of collaborative computing devices and applications is prohibited.
2552 2553		A.03.13.12.b: an explicit indication of use is provided to users who are physically present at the devices.
2554		ASSESSMENT METHODS AND OBJECTS
2555		Examine
2556 2557 2558 2559		[SELECT FROM: system and communications protection policy and procedures; procedures for collaborative computing; access control policy and procedures; system configuration settings; system design documentation; system audit records; system security plan; other relevant documents or records]
2560		Interview
2561 2562 2563		[SELECT FROM: personnel with responsibilities for managing collaborative computing devices; personnel with information security responsibilities; system developers; system administrators]
2564		Test
2565 2566 2567		[SELECT FROM: mechanisms supporting and/or implementing the management of remote activation of collaborative computing devices; mechanisms for providing an indication of use of collaborative computing devices]
2568		REFERENCES
2569		Source Assessment Procedure: SC-15

2570	3.13.13.	Mobile Code
2571		REQUIREMENT: 03.13.13
2572		ASSESSMENT OBJECTIVE
2573		Determine if:
2574		A.03.13.13.a[01]: acceptable mobile code is defined.
2575		A.03.13.13.a[02]: acceptable mobile code technologies are defined.
2576		A.03.13.13.b[01]: the use of mobile code is authorized.
2577		A.03.13.13.b[02]: the use of mobile code is monitored.
2578		A.03.13.13.b[03]: the use of mobile code is controlled.
2579		ASSESSMENT METHODS AND OBJECTS
2580		Examine
2581 2582 2583 2584		[SELECT FROM: system and communications protection policy and procedures; procedures for mobile code; mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; authorization records; system monitoring records; system audit records; system security plan; other relevant documents or records]
2585		Interview
2586 2587		[SELECT FROM: personnel with responsibilities for managing mobile code; personnel with information security responsibilities; system administrators]
2588		Test
2589 2590 2591		[SELECT FROM: processes for authorizing, monitoring, and controlling mobile code; mechanisms for supporting and/or implementing the management of mobile code; mechanisms for supporting and/or implementing mobile code monitoring]
2592		REFERENCES
2593		Source Assessment Procedure: <u>SC-18</u>
2594	3.13.14.	Withdrawn
2595		Technology-specific.
2596	3.13.15.	Session Authenticity
2597		REQUIREMENT: 03.13.15
2598		ASSESSMENT OBJECTIVE
2599		Determine if:
2600		A.03.13.15: the authenticity of communications sessions is protected.

2601		ASSESSMENT METHODS AND OBJECTS
2602		Examine
2603 2604 2605		[SELECT FROM: system and communications protection policy and procedures; procedures for session authenticity; system design documentation; system configuration settings; system audit records; system security plan; other relevant documents or records]
2606		Interview
2607		[SELECT FROM: personnel with information security responsibilities; system administrators]
2608		Test
2609		[SELECT FROM: mechanisms for supporting and/or implementing session authenticity]
2610		REFERENCES
2611		Source Assessment Procedure: <u>SC-23</u>
2612	3.13.16.	Withdrawn
2613		Incorporated into <u>03.13.08</u> .
2614	3.14. <u>S</u> y	ystem and Information Integrity
2615	3.14.1. F	Flaw Remediation
2616	F	REQUIREMENT: 03.14.01
2617	A	ASSESSMENT OBJECTIVE
2618	1	Determine if:
2619 2620		A.03.14.01.ODP[01]: time period within which to install security-relevant software updates is defined.
2621 2622		A.03.14.01.ODP[02]: time period within which to install security-relevant firmware updates is defined.
2623	A	A.03.14.01.a[01]: system flaws are identified.
2624	A	A.03.14.01.a[02]: system flaws are reported.
2625	A	A.03.14.01.a[03]: system flaws are corrected.
2626 2627		A.03.14.01.b[01]: security-relevant software updates are installed within <a.03.14.01.odp[01]. period="" time=""> of the release of the updates.</a.03.14.01.odp[01].>
2628 2629		A.03.14.01.b[02]: security-relevant firmware updates are installed within <a.03.14.01.odp[02] period="" time=""> of the release of the updates.</a.03.14.01.odp[02]>
2630		ASSESSMENT METHODS AND OBJECTS
2631	E	Examine
2632 2633 2634 2635	r	SELECT FROM: system and information integrity policy and procedures; procedures for flaw remediation; procedures for configuration management; list of recent security flaw remediation actions performed on the system; list of flaws and vulnerabilities that may potentially affect the system; test results from the installation of software and firmware updates to correct system

2636 flaws; installation and change control records for security-relevant software and firmware 2637 updates: system security plan; other relevant documents or records] 2638 Interview 2639 [SELECT FROM: personnel responsible for installing, configuring, and/or maintaining the 2640 system; personnel responsible for flaw remediation; personnel with configuration management 2641 responsibilities; personnel with information security responsibilities; system administrators] 2642 Test 2643 [SELECT FROM: processes for identifying, reporting, and correcting system flaws; processes 2644 for installing software and firmware updates; mechanisms for supporting and/or implementing 2645 the reporting and correction of system flaws; mechanisms for supporting and/or implementing 2646 the testing software and firmware updates] 2647 **REFERENCES** 2648 Source Assessment Procedure: SI-02 2649 3.14.2. Malicious Code Protection 2650 **REQUIREMENT: 03.14.02** 2651 ASSESSMENT OBJECTIVE 2652 Determine if: 2653 A.03.14.02.ODP[01]: the frequency at which malicious code protection mechanisms 2654 perform scans is defined. 2655 A.03.14.02.a[01]: malicious code protection mechanisms are implemented at designated 2656 locations within the system to detect malicious code. 2657 A.03.14.02.a[02]: malicious code protection mechanisms are implemented at designated 2658 locations within the system to eradicate malicious code. 2659 A.03.14.02.b: malicious code protection mechanisms are updated as new releases are 2660 available in accordance with configuration management policy and procedures. 2661 A.03.14.02.c.01[01]: malicious code protection mechanisms are configured to perform scans of 2662 the system < A.03.14.02.ODP[01]: the frequency>. 2663 A.03.14.02.c.01[02]: malicious code protection mechanisms are configured to perform real-time 2664 scans of files from external sources at endpoints or network entry and exit points as the files are 2665 downloaded, opened, or executed. 2666 A.03.14.02.c.02: malicious code protection mechanisms are configured to block malicious code, 2667 quarantine malicious code, or take other actions in response to malicious code detection. 2668 **ASSESSMENT METHODS AND OBJECTS** 2669 **Examine** 2670 [SELECT FROM: system and information integrity policy and procedures; configuration 2671 management policy and procedures; procedures for malicious code protection; records of 2672 malicious code protection updates; system design documentation; system configuration 2673 settings; scan results from malicious code protection mechanisms; record of actions initiated by 2674 malicious code protection mechanisms in response to malicious code detection; system audit 2675 records; system security plan; other relevant documents or records]

2676 Interview 2677 ISELECT FROM: personnel responsible for malicious code protection: personnel with system 2678 installation, configuration, and/or maintenance responsibilities; personnel with information 2679 security responsibilities; system administrators] 2680 **Test** 2681 [SELECT FROM: processes for employing, updating, and configuring malicious code protection 2682 mechanisms; processes for addressing the detection of false positives and resulting potential 2683 impacts; mechanisms for supporting and/or implementing, employing, updating, and configuring 2684 malicious code protection mechanisms; mechanisms for supporting and/or implementing 2685 malicious code scanning and the execution of subsequent actions] 2686 **REFERENCES** 2687 Source Assessment Procedure: SI-03 2688 3.14.3. Security Alerts, Advisories, and Directives 2689 **REQUIREMENT: 03.14.03** 2690 ASSESSMENT OBJECTIVE 2691 Determine if: 2692 A.03.14.03.a: system security alerts, advisories, and directives from external organizations are 2693 received on an ongoing basis. 2694 A.03.14.03.b[01]: internal security alerts, advisories, and directives are generated, as 2695 necessary. 2696 A.03.14.03.b[02]: internal security alerts, advisories, and directives are disseminated, as 2697 necessary. 2698 **A.03.14.03.c:** security directives are implemented in accordance with established time frames. 2699 ASSESSMENT METHODS AND OBJECTS 2700 **Examine** 2701 [SELECT FROM: system and information integrity policy and procedures; procedures for 2702 security alerts, advisories, and directives; records of security alerts and advisories; system 2703 security plan; other relevant documents or records] 2704 Interview 2705 [SELECT FROM: personnel with security alert and advisory responsibilities; personnel 2706 implementing, operating, maintaining, and using the system; personnel, organizational 2707 elements, and/or external organizations to whom alerts, advisories, and directives are to be 2708 disseminated: personnel with information security responsibilities: system administrators1 2709 Test 2710 [SELECT FROM: processes for defining, receiving, generating, disseminating, and complying 2711 with security alerts, advisories, and directives; mechanisms for supporting and/or implementing 2712 security directives; mechanisms for supporting and/or implementing the definition, receipt, 2713 generation, and dissemination of security alerts, advisories, and directives] 2714 **REFERENCES** 2715 Source Assessment Procedure: SI-05

2716	3.14.4.	Withdrawn
2717		Incorporated into <u>03.14.02</u> .
2718	3.14.5.	Withdrawn
2719		Addressed by <u>03.14.02</u> .
2720	3.14.6.	System Monitoring
2721		REQUIREMENT: 03.14.06
2722		ASSESSMENT OBJECTIVE
2723		Determine if:
2724		A.03.14.06.a.01: the system is monitored to detect attacks and indicators of potential attacks.
2725		A.03.14.06.a.02: the system is monitored to detect unauthorized connections.
2726		A.03.14.06.b: unauthorized use of the system is identified.
2727 2728		A.03.14.06.c[01]: inbound communications traffic is monitored to detect unusual or unauthorized activities or conditions.
2729 2730		A.03.14.06.c[02]: outbound communications traffic is monitored to detect unusual or unauthorized activities or conditions.
2731		ASSESSMENT METHODS AND OBJECTS
2732		Examine
2733 2734 2735 2736 2737		[SELECT FROM: system and information integrity policy and procedures; procedures for system monitoring tools and techniques; continuous monitoring strategy; facility diagram or layout; system design documentation; locations within the system where monitoring devices are deployed; system configuration settings; system protocols; system audit records; system security plan; other relevant documents or records]
2738		Interview
2739 2740 2741		[SELECT FROM: personnel with responsibilities for installing, configuring, and/or maintaining the system; personnel with system monitoring responsibilities; personnel with intrusion detection responsibilities; personnel with information security responsibilities; system administrators]
2742		Test
2743 2744 2745 2746		[SELECT FROM: processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing system monitoring capabilities; mechanisms for supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing the monitoring of inbound and outbound communications traffic
2747		REFERENCES
2748		Source Assessment Procedures: <u>SI-04</u> , <u>SI-04(04)</u>
2749	3.14.7.	Withdrawn
2750		Incorporated into <u>03.14.06</u> .

2751	3.14.8.	Information Management and Retention
2752		REQUIREMENT: 03.14.08
2753		ASSESSMENT OBJECTIVE
2754		Determine if:
2755 2756 2757		A.03.14.08[01]: CUI within the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.
2758 2759		A.03.14.08[02]: CUI within the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.
2760 2761 2762		A.03.14.08[03]: CUI output from the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.
2763 2764 2765		A.03.14.08[04]: CUI output from the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.
2766		ASSESSMENT METHODS AND OBJECTS
2767		Examine
2768 2769 2770 2771 2772		[SELECT FROM: system and information integrity policy and procedures; laws, Executive Orders, directives, policies, regulations, standards, and operational requirements applicable to information management and retention; records retention and disposition policy; records retention and disposition procedures; media protection policy; media protection procedures; audit findings; system security plan; other relevant documents or records]
2773		Interview
2774 2775 2776		[SELECT FROM: personnel with information and records management, retention, and disposition responsibilities; personnel with information security responsibilities; system administrators]
2777		Test
2778 2779 2780		[SELECT FROM: processes for information management, retention, and disposition; mechanisms for supporting and/or implementing information management, retention, and disposition]
2781		REFERENCES
2782		Source Assessment Procedure: <u>SI-12</u>
2783	3.15.	<u>Planning</u>
2784	3.15.1.	Policy and Procedures
2785		REQUIREMENT: 03.15.01
2786		ASSESSMENT OBJECTIVE
2787		Determine if:

2788 2789		A.03.15.01.a[01]: policies for implementing security requirements are developed and documented.
2790 2791		A.03.15.01.a[02]: policies for implementing security requirements are disseminated to organizational personnel or roles.
2792 2793		A.03.15.01.a[03]: procedures needed to implement security requirements are developed and documented.
2794 2795		A.03.15.01.a[04]: procedures needed to implement security requirements are disseminated to organizational personnel or roles.
2796		A.03.15.01.b[01]: policies and procedures are reviewed periodically.
2797		A.03.15.01.b[02]: policies and procedures are updated periodically.
2798		ASSESSMENT METHODS AND OBJECTS
2799		Examine
2800 2801		[SELECT FROM: security policies and procedures associated with the protection of CUI; audit findings; system security plan; other relevant documents or records]
2802		Interview
2803		[SELECT FROM: personnel with information security responsibilities]
2804		REFERENCES
2805 2806		Source Assessment Procedures: <u>AC-01</u> , <u>AT-01</u> , <u>AU-01</u> , <u>CA-01</u> , <u>CM-01</u> , <u>IA-01</u> , <u>IR-01</u> , <u>MA-01</u> <u>MP-01</u> , <u>PE-01</u> , <u>PL-01</u> , <u>PS-01</u> , <u>RA-01</u> , <u>SA-01</u> , <u>SC-01</u> , <u>SI-01</u> , <u>SR-01</u>
2807	3.15.2.	System Security Plan
2808		REQUIREMENT: 03.15.02
2809		ASSESSMENT OBJECTIVE
2809 2810		ASSESSMENT OBJECTIVE Determine if:
2810 2811		Determine if: A.03.15.02.a.01: a system security plan that defines the constituent system components is
2810 2811 2812 2813		 Determine if: A.03.15.02.a.01: a system security plan that defines the constituent system components is developed. A.03.15.02.a.02: a system security plan that describes the system operating environment is
2810 2811 2812 2813 2814 2815		 Determine if: A.03.15.02.a.01: a system security plan that defines the constituent system components is developed. A.03.15.02.a.02: a system security plan that describes the system operating environment is developed. A.03.15.02.a.03: a system security plan that describes any specific threats to the system that
2810 2811 2812 2813 2814 2815 2816 2817		 A.03.15.02.a.01: a system security plan that defines the constituent system components is developed. A.03.15.02.a.02: a system security plan that describes the system operating environment is developed. A.03.15.02.a.03: a system security plan that describes any specific threats to the system that are of concern to the organization is developed. A.03.15.02.a.04: a system security plan that provides an overview of the security requirements.
2810 2811 2812 2813 2814 2815 2816 2817 2818 2819		 A.03.15.02.a.01: a system security plan that defines the constituent system components is developed. A.03.15.02.a.02: a system security plan that describes the system operating environment is developed. A.03.15.02.a.03: a system security plan that describes any specific threats to the system that are of concern to the organization is developed. A.03.15.02.a.04: a system security plan that provides an overview of the security requirements for the system is developed. A.03.15.02.a.05: a system security plan that identifies connections to other systems is
2810 2811 2812 2813 2814 2815 2816 2817 2818 2819 2820 2821		 A.03.15.02.a.01: a system security plan that defines the constituent system components is developed. A.03.15.02.a.02: a system security plan that describes the system operating environment is developed. A.03.15.02.a.03: a system security plan that describes any specific threats to the system that are of concern to the organization is developed. A.03.15.02.a.04: a system security plan that provides an overview of the security requirements for the system is developed. A.03.15.02.a.05: a system security plan that identifies connections to other systems is developed. A.03.15.02.a.06: a system security plan that identifies individuals who fulfill system roles and
2810 2811 2812 2813 2814 2815 2816 2817 2818 2819 2820 2821 2822 2823		 A.03.15.02.a.01: a system security plan that defines the constituent system components is developed. A.03.15.02.a.02: a system security plan that describes the system operating environment is developed. A.03.15.02.a.03: a system security plan that describes any specific threats to the system that are of concern to the organization is developed. A.03.15.02.a.04: a system security plan that provides an overview of the security requirements for the system is developed. A.03.15.02.a.05: a system security plan that identifies connections to other systems is developed. A.03.15.02.a.06: a system security plan that identifies individuals who fulfill system roles and responsibilities is developed. A.03.15.02.a.07: a system security plan that includes other relevant information necessary for

2827 A.03.15.02.c: the system security plan is protected from unauthorized disclosure. 2828 **ASSESSMENT METHODS AND OBJECTS** 2829 Examine 2830 [SELECT FROM: security planning policy and procedures; procedures for system security plan 2831 development and implementation; procedures for security plan reviews and updates; enterprise 2832 architecture; system security plan; records of system security plan reviews and updates; risk 2833 assessments; risk assessment results; security architecture and design documentation; other 2834 relevant documents or records] 2835 Interview 2836 [SELECT FROM: personnel with system security planning and plan implementation 2837 responsibilities; system developers; personnel with information security responsibilities] 2838 2839 [SELECT FROM: processes for system security plan development, review, update, and 2840 approval] 2841 **REFERENCES** 2842 Source Assessment Procedure: PL-02 2843 3.15.3. Rules of Behavior 2844 REQUIREMENT: 03.15.03 2845 **ASSESSMENT OBJECTIVE** 2846 Determine if: 2847 A.03.15.03.a[01]: rules that describe responsibilities and expected behavior for handling CUI 2848 and system usage are established. 2849 A.03.15.03.a[02]: rules of behavior for handling CUI and system usage are provided to 2850 individuals who require access to the system. 2851 A.03.15.03.b: a documented acknowledgement from individuals indicating that they have read, 2852 understand, and agree to abide by the rules of behavior is received before authorizing access to 2853 CUI and the system. 2854 **A.03.15.03.c[01]:** the rules of behavior are reviewed periodically. 2855 A.03.15.03.c[02]: the rules of behavior are updated periodically. 2856 ASSESSMENT METHODS AND OBJECTS 2857 **Examine** 2858 [SELECT FROM: security planning policy and procedures; rules of behavior for system users; 2859 signed acknowledgements of rules of behavior; records for rules of behavior reviews and 2860 updates; system security plan; other relevant documents or records] 2861 Interview 2862 [SELECT FROM: personnel with rules of behavior establishment, review, and update 2863 responsibilities; personnel with literacy training and awareness responsibilities; personnel with 2864 role-based training responsibilities; authorized users of the system who have signed rules of 2865 behavior; personnel with information security responsibilities]

2866		Test
2867 2868 2869		[SELECT FROM: processes for establishing, reviewing, disseminating, and updating rules of behavior; mechanisms for supporting and/or implementing the establishment, dissemination, review, and update of rules of behavior]
2870		REFERENCES
2871		Source Assessment Procedure: <u>PL-04</u>
2872	3.16.	System and Services Acquisition
2873	3.16.1.	Acquisition Process
2874		REQUIREMENT: 03.16.01
2875		ASSESSMENT OBJECTIVE
2876		Determine if:
2877 2878		A.03.16.01.ODP[01]: the security requirements for the system, system component, or system service are defined.
2879 2880 2881		A.03.16.01: the following security requirements are included in the acquisition contract for the system, system component, or system service: A.03.16.01.ODP[01] : security requirements>.
2882		ASSESSMENT METHODS AND OBJECTS
2883		Examine
2884 2885 2886 2887 2888		[SELECT FROM: system and services acquisition policy and procedures; procedures for the integration of information security and SCRM into the acquisition process; configuration management plan; acquisition contracts for the system, system component, or system service; system design documentation; SCRM plan; system security plan; other relevant documents or records]
2889		Interview
2890 2891		[SELECT FROM: personnel with acquisition/contracting responsibilities; personnel with SCRM responsibilities; personnel with information security responsibilities; system administrators]
2892		Test
2893 2894 2895		[SELECT FROM: processes for determining system security requirements; processes for developing acquisition contracts; mechanisms for supporting and/or implementing acquisitions and the inclusion of security requirements in contracts]
2896		REFERENCES
2897		Source Assessment Procedure: <u>SA-04</u>
2898	3.16.2.	Unsupported System Components
2899		REQUIREMENT: 03.16.02

2900		ASSESSMENT OBJECTIVE
2901		Determine if:
2902 2903		A.03.16.02.a: system components are replaced when support for the components is no longer available from the developer, vendor, or manufacturer.
2904 2905		A.03.16.02.b: options for risk mitigation or alternative sources for continued support for unsupported components are provided if components cannot be replaced.
2906		ASSESSMENT METHODS AND OBJECTS
2907		Examine
2908 2909 2910 2911 2912		[SELECT FROM: system and services acquisition policy and procedures; procedures for the replacement or continued use of unsupported system components; documented evidence of replacing unsupported system components; documented approvals (including justification) for the continued use of unsupported system components; SCRM plan; system security plan; other relevant documents or records]
2913		Interview
2914 2915 2916		[SELECT FROM: personnel with system and service acquisition responsibilities; personnel responsible for component replacement; personnel with system development life cycle responsibilities; personnel with information security responsibilities]
2917		Test
2918 2919		[SELECT FROM: processes for replacing unsupported system components; mechanisms for supporting and/or implementing the replacement of unsupported system components]
2920		REFERENCES
2921		Source Assessment Procedure: <u>SA-22</u>
2922	3.16.3.	External System Services
2923		REQUIREMENT: 03.16.03
2924		ASSESSMENT OBJECTIVE
2925		Determine if:
2926 2927		A.03.16.03.ODP[01]: the security requirements to be employed by external system service providers are defined.
2928 2929 2930		A.03.16.03.a : the providers of external system services used for the processing, storage, or transmission of CUI comply with the following security requirements: < A.03.16.03.ODP[01] : security requirements>.
2931 2932		A.03.16.03.b: user roles and responsibilities with regard to external system services, including shared responsibilities with external providers, are defined and documented.
2933 2934		A.03.16.03.c: processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.
2935		ASSESSMENT METHODS AND OBJECTS
2936		Examine
2937 2938		[SELECT FROM: system and services acquisition policy and procedures; procedures for monitoring security requirement compliance by external service providers; acquisition

2939 2940 2941 2942		documentation; contracts; service-level agreements; interagency agreements; licensing agreements; list of security requirements for external provider services; assessment results or reports from external service providers; SCRM plan; system security plan; other relevant documents or records]
2943		Interview
2944 2945 2946		[SELECT FROM: personnel with acquisition responsibilities; external providers of system services; personnel with SCRM responsibilities; personnel with information security responsibilities]
2947		Test
2948 2949 2950		[SELECT FROM: organizational processes for monitoring security and privacy control compliance by external service providers on an ongoing basis; mechanisms for monitoring security and privacy control compliance by external service providers on an ongoing basis]
2951		REFERENCES
2952		Source Assessment Procedure: <u>SA-09</u>
2953	3.17.	Supply Chain Risk Management
2954	3.17.1	. Supply Chain Risk Management Plan
2955		REQUIREMENT: 03.17.01
2956		ASSESSMENT OBJECTIVE
2957		Determine if:
2958		A.03.17.01.a[01]: a plan for managing supply chain risks is developed.
2959 2960		A.03.17.01.a[02]: the SCRM plan addresses risks associated with the research and development of the system, system components, or system services.
2961 2962		A.03.17.01.a[03]: the SCRM plan addresses risks associated with the design of the system, system components, or system services.
2963 2964		A.03.17.01.a[04]: the SCRM plan addresses risks associated with the manufacturing of the system, system components, or system services.
2965 2966		A.03.17.01.a[05]: the SCRM plan addresses risks associated with the acquisition of the system, system components, or system services.
2967 2968		A.03.17.01.a[06]: the SCRM plan addresses risks associated with the delivery of the system, system components, or system services.
2969 2970		A.03.17.01.a[07]: the SCRM plan addresses risks associated with the integration of the system, system components, or system services.
2971 2972		A.03.17.01.a[08]: the SCRM plan addresses risks associated with the operations and maintenance of the system, system components, or system services.
2973 2974		A.03.17.01.a[09]: the SCRM plan addresses risks associated with the disposal of the system, system components, or system services.
2975		A.03.17.01.b[01]: the SCRM plan is reviewed periodically.
2976		A.03.17.01.b[02]: the SCRM plan is updated periodically.
2977		A.03.17.01.c: the SCRM plan is protected from unauthorized disclosure.

2978 **ASSESSMENT METHODS AND OBJECTS** 2979 **Examine** 2980 ISELECT FROM: SCRM policy and procedures: SCRM plan: system and services acquisition 2981 policy and procedures; system and services acquisition procedures; procedures for supply 2982 chain protection; procedures for protecting the SCRM plan from unauthorized disclosure; 2983 system development life cycle procedures; procedures for the integration of information security 2984 requirements into the acquisition process; acquisition documentation; service-level agreements; 2985 acquisition contracts for the system, system components, or system services; list of supply 2986 chain threats; list of safeguards for supply chain threats; system life cycle documentation; inter-2987 organizational agreements and procedures; system security plan; other relevant documents or 2988 records] 2989 Interview 2990 [SELECT FROM: personnel with acquisition responsibilities; personnel with SCRM 2991 responsibilities; personnel with information security responsibilities] 2992 2993 [SELECT FROM: organizational processes for defining and documenting the system 2994 development life cycle (SDLC); organizational processes for identifying SDLC roles and 2995 responsibilities; organizational processes for integrating SCRM into the SDLC; mechanisms for 2996 supporting and/or implementing the SDLC1 2997 **REFERENCES** 2998 Source Assessment Procedure: SR-02 2999 3.17.2. Acquisition Strategies, Tools, and Methods 3000 **REQUIREMENT: 03.17.02** 3001 ASSESSMENT OBJECTIVE 3002 Determine if: 3003 A.03.17.02[01]: acquisition strategies, contract tools, and procurement methods are developed 3004 and implemented to identify supply chain risks. 3005 A.03.17.02[02]: acquisition strategies, contract tools, and procurement methods are developed 3006 and implemented to protect against supply chain risks. 3007 A.03.17.02[03]: acquisition strategies, contract tools, and procurement methods are developed 3008 and implemented to mitigate supply chain risks. 3009 ASSESSMENT METHODS AND OBJECTS 3010 **Examine** 3011 [SELECT FROM: SCRM policy and procedures; SCRM plan; system and services acquisition 3012 policy and procedures; procedures for supply chain protection; procedures for the integration of 3013 information security requirements into the acquisition process; solicitation documentation: 3014 acquisition documentation (including purchase orders); service-level agreements; acquisition 3015 contracts for the system, system components, or services; documentation of training, education, 3016 and awareness programs for personnel regarding supply chain risk; system security plan; other 3017 relevant documents or records]

3018 Interview 3019 ISELECT FROM: personnel with acquisition responsibilities; personnel with SCRM 3020 responsibilities; personnel with information security responsibilities] 3021 3022 [SELECT FROM: processes for defining and employing tailored acquisition strategies, contract 3023 tools, and procurement methods; mechanisms for supporting and/or implementing the definition 3024 and employment of tailored acquisition strategies, contract tools, and procurement methods] 3025 **REFERENCES** 3026 Source Assessment Procedure: SR-05 3027 3.17.3. Supply Chain Requirements and Processes 3028 REQUIREMENT: 03.17.03 3029 **ASSESSMENT OBJECTIVE** 3030 Determine if: 3031 A.03.17.03.ODP[01]: the security requirements to protect against supply chain risks to 3032 the system, system components, or system services and to limit the harm or 3033 consequences from supply chain-related events are defined. 3034 A.03.17.03.a: a process for identifying and addressing weaknesses or deficiencies in the supply 3035 chain elements and processes is established. 3036 A.03.17.03.b: the following security requirements are enforced to protect against supply chain 3037 risks to the system, system components, or system services and to limit the harm or 3038 consequences of supply chain-related events: < A.03.17.03.ODP[01]: security requirements>. 3039 ASSESSMENT METHODS AND OBJECTS 3040 **Examine** 3041 [SELECT FROM: SCRM policy and procedures; SCRM strategy; SCRM plan; systems and 3042 critical system components inventory documentation; system and services acquisition policy 3043 and procedures; procedures for the integration of security requirements into the acquisition 3044 process; solicitation documentation; acquisition documentation (including purchase orders); 3045 acquisition contracts for systems or services; service-level agreements; risk register 3046 documentation; system security plan; other relevant documents or records] 3047 Interview 3048 [SELECT FROM: personnel with acquisition responsibilities; personnel with information security 3049 responsibilities; personnel with SCRM responsibilities] 3050 **Test** 3051 [SELECT FROM: processes for identifying and addressing supply chain element and process 3052 deficiencies] 3053 **REFERENCES** 3054 Source Assessment Procedure: SR-03

3055 References

- 3056 [1] Federal Information Security Modernization Act (P.L. 113-283), December 2014. Available at https://www.govinfo.gov/app/details/PLAW-113publ283
- 3058 [2] Office of Management and Budget Memorandum Circular A-130, Managing Information as a Strategic Resource, July 2016. Available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
- 3061 [3] Ross RS, Pillitteri VY (2023) 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 ipd, initial public draft.

 3064 https://doi.org/10.6028/NIST.SP.800-171r3.ipd
- Joint Task Force Transformation Initiative (2011) Managing Information Security Risk:
 Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
 https://doi.org/10.6028/NIST.SP.800-39
- Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53A75
- [6] International Organization for Standardization/International Electrotechnical Commission
 15408-3:2017, Information technology Security techniques Evaluation criteria for IT
 security Part 3: Security assurance requirements, April 2017.
 https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf
- 3077 [7] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3.

 https://doi.org/10.6028/NIST.FIPS.140-3
- 3081 [8] Committee on National Security Systems (2022) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm
- 3084 [9] Executive Order 13556 (2010) Controlled Unclassified Information. (The White House, 2340 Washington, DC), DCPD-201000942, November 4, 2010. Available at https://www.govinfo.gov/app/details/DCPD-201000942

3087	Appendix A. Acronyms
3088 3089	CNSS Committee on National Security Systems
3090 3091	CUI Controlled Unclassified Information
3092 3093	FIPS Federal Information Processing Standards
3094 3095	FISMA Federal Information Security Modernization Act
3096 3097	GRC Governance, Risk, and Compliance
3098 3099	ODP Organization-Defined Parameter
3100 3101	OMB Office of Management and Budget
3102 3103	OSCAL Open Security Controls Assessment Language
3104 3105	SCRM Supply Chain Risk Management
3106 3107	SDLC System Development Life Cycle
3108 3109	SP Special Publication

3110	Appendix B. Glossary
3111 3112 3113	Appendix B provides definitions for the terminology used in NIST SP 800-171A. The definitions are consistent with the definitions contained in the Committee on National Security Systems (CNSS) Glossary [8] unless otherwise noted.
3114 3115 3116 3117	agency Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency. [2]
3118 3119	assessment See security control assessment.
3120 3121	assessor See security control assessor.
3122 3123 3124 3125	controlled unclassified information Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. [9]
3126 3127 3128	information Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. [2]
3129 3130	nonfederal organization An entity that owns, operates, or maintains a nonfederal system.
3131 3132	nonfederal system A system that does not meet the criteria for a federal system.
3133 3134 3135 3136	risk A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [2]
3137 3138 3139 3140 3141	security A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach. [8]
3142 3143	security assessment See security control assessment.
3144 3145 3146	security control The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. [2]
3147 3148 3149 3150	security control assessment The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. [2]

3151	system
------	--------

3152 See information system.

3153 system security plan

- A document that describes how an organization meets the security requirements for a system or plans to meet the requirements. In particular, the system security plan describes the system boundary, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other
- 3157 systems.

Appendix C. Change Log

3158

- 3159 This publication incorporates the following changes from the original edition (June 2018):
- Assessment procedures have been updated to be consistent with NIST SP 800-171, Revision 3 [3].
- Organization-defined parameters (ODPs) have been added to determination statements.
- A references section has been added to each assessment procedure providing a hyperlink to the source assessment procedure in NIST SP 800-53A [5].
- Table 2 shows the changes incorporated into this publication. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature. Any potential updates to this document that are not yet published in an errata update or a formal revision, including additional issues and potential corrections, will be posted as they are identified. See the publication details for this report. The current release of this publication does not include any errata updates.

3171

Table 2. Change Log

Publication ID	Date	Type of Edit	Change	Location