Unofficial Markup SP 800-53, Revision 4, Appendix D

This document provides an unofficial markup comparing SP 800-53, Revision 4, Appendix D (Final Public Draft) to the Initial Public Draft of Revision 4. Upon final publication of SP 800-53, Revision 4 in April 2013, NIST will publish a final markup of Appendix D providing changes from Revision 3 to Revision 4. Organizations should refer to SP 800-53, Revision 4 (clean copy) as the official source publication in situations where there are inconsistencies or discrepancies noted in the markup version.

APPENDIX D

SECURITY CONTROL BASELINES – SUMMARY

LOW-IMPACT, MODERATE-IMPACT, AND HIGH-IMPACT INFORMATION SYSTEMS

This appendix contains the security control baselines that represent the *starting point* in determining the security controls for low-impact, moderate-impact, and high-impact information systems.[1] The three security control baselines are hierarchical in nature with regard to the security controls employed in those baselines.[2] If a security control is selected for one of the baselines, the family identifier and control number are listed in the appropriate column. If a security control is not used in a particular baseline, the entry is marked *not selected*. Security control enhancements, when used to supplement security controls, are indicated by the number of the enhancement. For example, an IR-2 (1) in the high baseline entry for the IR-2 security control indicates that the second control from the Incident Response family has been selected along with control enhancement (1). Some security controls and enhancements in the security control catalog are not used in any of the baselines in this appendix but are available for use by organizations if needed. This situation occurs, for example, when the results of a risk assessment indicate the need for additional security controls or control enhancements in order to adequately mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

Organizations can use the recommended *priority code* designation associated with each security control in the baselines to assist in making sequencing decisions for control implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control; a Priority Code 2 [P2] control has a higher priority for implementation than a Priority Code 3 [P3] control, and a Priority Code 0 [P0] indicates the security control is not selected in any baseline). This recommended sequencing prioritization helps ensure that security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources. The implementation of security controls by sequence priority code does not imply any defined level of risk mitigation until *all* controls in the security plan have been implemented. The priority codes are used only for implementation sequencing, not for making security control selection decisions. Table D-1 summarizes sequence priority codes for the baseline security controls in Table D-2.

Deleted:).

TABLE D-1: SECURITY CONTROL PRIORITIZATION CODES

Priority Code	Sequencing	Action
Priority Code 1 (P1)	FIRST	Implement P1 security controls first.
Priority Code 2 (P2)	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 (P3)	LAST	Implement P3 security controls after implementation of P1 and P2 controls.

[1] A complete description of all security controls is provided in Appendices F and G. In addition, separate documents for individual security control baselines (listed as Annexes 1, 2, and 3) are available at http://csrc.nist.gov/publications. An online version of the catalog of security controls is also available at http://web.nvd.nist.gov/view/800-53/home.

[2] The hierarchical nature applies to the security requirements of each control (i.e., the base control plus all of its enhancements) at the low-impact, moderate-impact, and high-impact level in that the control requirements at a particular impact level (e.g., CP-4 *Contingency Plan Testing*—Moderate: CP-4 (1)) meets a stronger set of security requirements for that control than the next lower impact level of the same control (e.g., CP-4 *Contingency Plan Testing*—Low: CP-4).

Unspecified Priority Code (P0)	NONE	Security control not selected in any baseline.

Table D-2 provides a summary of the security controls and control enhancements from Appendix F that have been allocated to the initial security control baselines (i.e., low, moderate, and high). The sequence priority codes for security control implementation and those security controls that have been withdrawn from Appendix F are also indicated in Table D-2. In addition to Table D-2, the sequence priority codes and security control baselines are annotated in a priority and baseline allocation summary section below each security control in Appendix F.

TABLE D-2: SECURITY CONTROL BASELINES[3]

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	**Withdrawn**	---	---	---	---
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P1	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P0	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P2	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected

[3] The security control baselines in Table D-2 are the initial baselines selected by organizations prior to conducting the tailoring activities described in Section 3.2. The control baselines and priority codes are only applicable to non-national security systems. Security control baselines for national security systems are included in CNSS Instruction 1253.

Deleted: for

Deleted: Login

Deleted: 6

Deleted: 6

Deleted: Collaboration and

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	**Withdrawn**	---	---	---	---
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	P1	Not Selected	Not Selected	Not Selected
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1) (3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	**Withdrawn**	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P3	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P3	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P1	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P1	CA-9	CA-9	CA-9
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3	CM-3 (1)
CM-4	Security Impact Analysis	P2	CM-4	CM-4 (3)	CM-4 (1) (3)

Deleted: Function

Moved down [3]: Not Selected

Moved (insertion) [1]

Moved down [2]: Contacts with Security Groups and Associations

Deleted: P3

Deleted: AT-5

Deleted: AT-5

Deleted: Auditable

Deleted: (4)

Deleted: (4)

Deleted: (9)

Deleted: (9)

Moved (insertion) [3]

Deleted: AU-10

Deleted: Information

Deleted: Connections

Deleted: 6

Deleted: (2)

Deleted: (2)

Deleted: Not Selected

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P1	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11
Contingency Planning					
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	P1	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	P2	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	**Withdrawn**	---	---	---	---
CP-6	Alternate Storage Site	P1	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	P1	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	P1	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	P1	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and Reconstitution	P1	CP-10	CP-10 (2)	CP-10 (2) (4)
CP-11	Alternate Communications Protocols	P0	Not Selected	Not Selected	Not Selected
CP-12	Safe Mode	P0	Not Selected	Not Selected	Not Selected
CP-13	Alternative Security Mechanisms	P0	Not Selected	Not Selected	Not Selected
Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (13)	IA-2 (1) (2) (3) (8) (11) (12) (13)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12) (13)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Authenticator Feedback	P1	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IA-9	Service Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-10	Adaptive Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-11	Re-authentication	P0	Not Selected	Not Selected	Not Selected
Incident Response					
IR-1	Incident Response Policy and Procedures	P1	IR-1	IR-1	IR-1

Deleted: (4)

Deleted: (3)

Deleted: 3) (

Deleted: (5)

Moved (insertion) [4]

Moved down [5]: Predictable Failure Prevention

Moved (insertion) [6]

Deleted: P1

Deleted: CP-11

Moved (insertion) [7]

Moved up [4]: Alternate Communications Protocols

Moved up [7]: Safe Mode

Deleted: Device-to-

Deleted: IA-10 ...

Moved up [6]: Not Selected

Deleted: 11

Deleted: 12

Deleted: Reauthentication

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	Incident Monitoring	P1	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	P3	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	P1	IR-8	IR-8	IR-8
IR-9	Information Spillage Response	P0	Not Selected	Not Selected	Not Selected
IR-10	Integrated Information Security Cell	P0	Not Selected	Not Selected	Not Selected
Maintenance					
MA-1	System Maintenance Policy and Procedures	P1	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	P2	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools	P2	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	P1	MA-4	MA-4 (2)	MA-4 (2) (3)
MA-5	Maintenance Personnel	P1	MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance	P1	Not Selected	MA-6	MA-6
Media Protection					
MP-1	Media Protection Policy and Procedures	P1	MP-1	MP-1	MP-1
MP-2	Media Access	P1	MP-2	MP-2	MP-2
MP-3	Media Marking	P1	Not Selected	MP-3	MP-3
MP-4	Media Storage	P1	Not Selected	MP-4	MP-4
MP-5	Media Transport	P1	Not Selected	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	P1	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	Media Use	P1	MP-7	MP-7 (1)	MP-7 (1)
MP-8	Media Downgrading	P0	Not Selected	Not Selected	Not Selected
Physical and Environmental Protection					
PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	P1	PE-2	PE-2	PE-2
PE-3	Physical Access Control	P1	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	P1	Not Selected	PE-4	PE-4
PE-5	Access Control for Output Devices	P1	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	P1	PE-6	PE-6 (1)	PE-6 (1) (4)
PE-7	**Withdrawn**	---	---	---	---
PE-8	Visitor Access Records	P3	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling	P1	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	P1	Not Selected	PE-10	PE-10
PE-11	Emergency Power	P1	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	P1	PE-12	PE-12	PE-12
PE-13	Fire Protection	P1	PE-13	PE-13 (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	P1	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	P1	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	P1	PE-16	PE-16	PE-16

Deleted: 1) (

Deleted: Non-Local

Deleted: 1) (

Deleted: 1) (

Deleted: (1)

Deleted: (1)

Deleted: 3) (

Deleted: (2)

Deleted: (2)

Deleted: 2

Deleted: 1) (2) (

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
PE-17	Alternate Work Site	P1	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P2	Not Selected	Not Selected	PE-18
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
Planning					
PL-1	Security Planning Policy and Procedures	P1	PL-1	PL-1	PL-1
PL-2	System Security Plan	P1	PL-2	PL-2 (3)	PL-2 (3)
PL-3	**Withdrawn**	---	---	---	---
PL-4	Rules of Behavior	P1	PL-4	PL-4 (1)	PL-4 (1)
PL-5	**Withdrawn**	---	---	---	---
PL-6	**Withdrawn**	---	---	---	---
PL-7	Security Concept of Operations	P0	Not Selected	Not Selected	Not Selected
PL-8	Information Security Architecture	P0	Not Selected	PL-8	PL-8
PL-9	Central Management	P0	Not Selected	Not Selected	Not Selected
Personnel Security					
PS-1	Personnel Security Policy and Procedures	P1	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	P1	PS-2	PS-2	PS-2
PS-3	Personnel Screening	P1	PS-3	PS-3	PS-3
PS-4	Personnel Termination	P2	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	P2	PS-5	PS-5	PS-5
PS-6	Access Agreements	P3	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	P1	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	P3	PS-8	PS-8	PS-8
Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3
RA-4	**Withdrawn**	---	---	---	---
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)
RA-6	Technical Surveillance Countermeasures Survey	P0	Not Selected	Not Selected	Not Selected
System and Services Acquisition					
SA-1	System and Services Acquisition Policy and Procedures	P1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	P1	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	P1	SA-3	SA-3	SA-3
SA-4	Acquisition Process	P1	SA-4 (10)	SA-4 (1) (2) (10)	SA-4 (1) (2) (10)
SA-5	Information System Documentation	P2	SA-5	SA-5	SA-5
SA-6	**Withdrawn**	---	---	---	---
SA-7	**Withdrawn**	---	---	---	---
SA-8	Security Engineering Principles	P1	Not Selected	SA-8	SA-8
SA-9	External Information System Services	P1	SA-9	SA-9 (2)	SA-9 (2)
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10

Deleted: PE-18 (1)

Deleted: (1)

Deleted: PE-20 ...

Moved (insertion) [8]

Deleted: 8

Deleted: Security Architecture

Deleted: Categorization

Deleted: 1) (

Deleted: (1)

Deleted: (1)

Deleted: (1)

Deleted: (1)

Deleted: 3) (

Deleted: (7)

Moved (insertion) [9]

Moved (insertion) [10]

Deleted: 4

Deleted: 4

Deleted: (1) (3) (6)

Deleted: (1) (2) (3) (6)

Deleted: (3)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SA-11	Developer Security Testing and Evaluation	P2	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P1	Not Selected	Not Selected	Not Selected
SA-14	Criticality Analysis	P0	Not Selected	Not Selected	Not Selected
SA-15	Development Process, Standards, and Tools	P2	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	P2	Not Selected	Not Selected	SA-16
SA-17	Developer Security Architecture and Design	P1	Not Selected	Not Selected	SA-17
SA-18	Tamper Resistance and Detection	P0	Not Selected	Not Selected	Not Selected
SA-19	Component Authenticity	P0	Not Selected	Not Selected	Not Selected
SA-20	Customized Development of Critical Components	P0	Not Selected	Not Selected	Not Selected
SA-21	Developer Screening	P0	Not Selected	Not Selected	Not Selected
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Availability	P0	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (21)
SC-8	Transmission Confidentiality and Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	Withdrawn	---	---	---	---
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	P1	SC-13	SC-13	SC-13
SC-14	Withdrawn	---	---	---	---
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P1	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected

Moved up [1]: Withdrawn
Deleted: ---
Deleted: ---
Deleted: ---
Deleted: ---
Deleted: Critical Information System Components
Deleted: Anti-Counterfeit
Deleted: (6)
Deleted: 1) (
Deleted: 1) (
Deleted: 6) (
Moved (insertion) [11]
Deleted: Transmission Confidentiality
Deleted: P1
Moved up [8]: Not Selected
Deleted: SC-9 (1)
Deleted: SC-9 (1)
Deleted: Public Access Protections
Deleted: P1
Deleted: SC-14
Deleted: SC-14
Deleted: SC-14

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	P0	Not Selected	Not Selected	Not Selected
SC-30	Concealment and Misdirection	P0	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	P0	Not Selected	Not Selected	Not Selected
SC-32	Information System Partitioning	P1	Not Selected	Not Selected	Not Selected
SC-33	**Withdrawn**	---	---	---	---
SC-34	Non-Modifiable Executable Programs	P0	Not Selected	Not Selected	Not Selected
SC-35	Honeyclients	P0	Not Selected	Not Selected	Not Selected
SC-36	Distributed Processing and Storage	P0	Not Selected	Not Selected	Not Selected
SC-37	Out-of-Band Channels	P0	Not Selected	Not Selected	Not Selected
SC-38	Operations Security	P0	Not Selected	Not Selected	Not Selected
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39
SC-40	Wireless Link Protection	P0	Not Selected	Not Selected	Not Selected
SC-41	Port and I/O Device Access	P0	Not Selected	Not Selected	Not Selected
SC-42	Sensor Data	P0	Not Selected	Not Selected	Not Selected
SC-43	Usage Restrictions	P0	Not Selected	Not Selected	Not Selected
SC-44	Detonation Chambers	P0	Not Selected	Not Selected	Not Selected
System and Information Integrity					
SI-1	System and Information Integrity Policy and Procedures	P1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	P1	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring	P1	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	P1	Not Selected	Not Selected	SI-6
SI-7	Software, Firmware, and Information Integrity	P1	Not Selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection	P1	Not Selected	SI-8 (1) (2)	SI-8 (1) (2)
SI-9	**Withdrawn**	---	---	---	---
SI-10	Information Input Validation	P1	Not Selected	SI-10	SI-10
SI-11	Error Handling	P2	Not Selected	SI-11	SI-11
SI-12	Information Handling and Retention	P2	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	P0	Not Selected	Not Selected	Not Selected
SI-14	Non-Persistence	P0	Not Selected	Not Selected	Not Selected
SI-15	Information Output Filtering	P0	Not Selected	Not Selected	Not Selected
SI-16	Memory Protection	P1	Not Selected	SI-16	SI-16
Program Management					
PM-1	Information Security Program Plan	P1	**Deployed organization-wide. Supporting information security program. Not associated with security control baselines.**		
PM-2	Senior Information Security Officer	P1			
PM-3	Information Security Resources	P1			
PM-4	Plan of Action and Milestones Process	P1			
PM-5	Information System Inventory	P1			

Deleted: Operating System
Deleted: SC-32
Deleted: SC-32
Moved (insertion) [12] ...
Moved up [9]: Technical Surveillance ...
Moved (insertion) [13] ...
Moved up [12]: Honeyclients
Moved (insertion) [14] ...
Moved up [13]: Distributed Processing and ...
Moved (insertion) [15] ...
Deleted: Malware Analysis
Moved (insertion) [16] ...
Deleted: 39
Moved (insertion) [17] ...
Moved up [14]: Out-of-Band Channels
Deleted: 40
Moved up [15]: Operations Security
Deleted: 41
Moved up [16]: Process Isolation
Deleted: P1
Deleted: SC-41
Deleted: SC-41
Deleted: SC-41
Deleted: 42
Moved up [17]: Wireless Link Protection
Deleted: ¶
Deleted: (3)
Deleted: (3)
Deleted: (6)
Deleted: (6)
Deleted: 8
Deleted: 8) (15
Deleted: Information Input Restrictions
Deleted: P2
Moved up [10]: Not Selected
Deleted: SI-9
Deleted: SI-9
Deleted: Output
Moved (insertion) [5] ...
Moved up [11]: Withdrawn
Deleted: ---
Deleted: ---
Deleted: ---
Deleted: ---
Deleted: ¶ ...
Deleted: all

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
PM-6	Information Security Measures of Performance	P1	Independent of any system impact level.		
PM-7	Enterprise Architecture	P1			
PM-8	Critical Infrastructure Plan	P1			
PM-9	Risk Management Strategy	P1			
PM-10	Security Authorization Process	P1			
PM-11	Mission/Business Process Definition	P1			
PM-12	Insider Threat Program	P1	Deployed organization-wide. Supporting information security program. Not associated with security control baselines. Independent of any system impact level.		
PM-13	Information Security Workforce	P1			
PM-14	Testing, Training, and Monitoring	P1			
PM-15	Contacts with Security Groups and Associations	P3			
PM-16	Threat Awareness Program	P1			

Deleted: ¶
¶

Deleted: PM-14 ...

Deleted: 15

Moved (insertion) [2]

Tables D-3 through D-19 provide a more detailed summary of the security controls and control enhancements in Appendix F. Each table focuses on a different security control family. Whereas Table D-2 includes only those security controls and control enhancements allocated to the three security control baselines, Tables D-3 through D-19 include all controls and enhancements for the respective security control families. The tables include the following information: (i) the security controls and control enhancements have been selected for each of the security control baselines;[4] (ii) the security controls and control enhancements have not been selected for any security control baseline (i.e., the controls and enhancements available for selection to achieve greater protection); (iii) the security controls and control enhancements that have been withdrawn from Appendix F; and (iv) the security controls and control enhancements that have assurance-related characteristics or properties (i.e., assurance-related controls). Assurance-related controls are discussed in greater detail in Appendix E to include the allocation of such controls to security control baselines (see Tables E-1 through E-3).

TABLE D-3: SUMMARY — ACCESS CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-1	**Access Control Policy and Procedures**		x	x	x	x
AC-2	**Account Management**			x	x	x
AC-2 (1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*				x	x
AC-2 (2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*				x	x
AC-2 (3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*				x	x
AC-2 (4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*				x	x
AC-2 (5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT*					x
AC-2 (6)	*ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT*					
AC-2 (7)	*ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES*					
AC-2 (8)	*ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION*					
AC-2 (9)	*ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS*					
AC-2 (10)	*ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION*					
AC-2 (11)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*					x
AC-2 (12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*					
AC-2 (13)	*ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS*					
AC-3	**Access Enforcement**			x	x	x
AC-3 (1)	*ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS*	x	Incorporated into AC-6.			
AC-3 (2)	*ACCESS ENFORCEMENT | DUAL AUTHORIZATION*					
AC-3 (3)	*ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL*					
AC-3 (4)	*ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL*					
AC-3 (5)	*ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION*					
AC-3 (6)	*ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION*	x	Incorporated into MP-4 and SC-28.			

[4] The security control baselines in Tables D-3 through D-19 are only applicable to non-national security systems. Security control baselines for national security systems are included in CNSS Instruction 1253.

Deleted: The following tables (
Deleted:)
Deleted: all
Deleted: by
Deleted: and name. The tables also illustrate: (i) the allocation of
Deleted: to
Deleted: : (ii)
Deleted: iii)
Deleted: A
Deleted: / *TYPICAL USAGE MONITORING*
Deleted: AC-2 (10)
Deleted: 11
Deleted: *RENEWALS*
Deleted: 12
Deleted: AC-2 (13)
Deleted: 14
Deleted: 15
Deleted: W
Deleted: *NONDISCRETIONARY*
Deleted: W

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-3 (7)	*ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL*					
AC-3 (8)	*ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS*					
AC-3 (9)	*ACCESS ENFORCEMENT | CONTROLLED RELEASE*					
AC-3 (10)	*ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS*					
AC-4	**Information Flow Enforcement**				x	x
AC-4 (1)	*INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY ATTRIBUTES*					
AC-4 (2)	*INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS*					
AC-4 (3)	*INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL*					
AC-4 (4)	*INFORMATION FLOW ENFORCEMENT | CONTENT CHECK ENCRYPTED INFORMATION*					
AC-4 (5)	*INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES*					
AC-4 (6)	*INFORMATION FLOW ENFORCEMENT | METADATA*					
AC-4 (7)	*INFORMATION FLOW ENFORCEMENT | ONE-WAY FLOW MECHANISMS*					
AC-4 (8)	*INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTERS*					
AC-4 (9)	*INFORMATION FLOW ENFORCEMENT | HUMAN REVIEWS*					
AC-4 (10)	*INFORMATION FLOW ENFORCEMENT | ENABLE / DISABLE SECURITY POLICY FILTERS*					
AC-4 (11)	*INFORMATION FLOW ENFORCEMENT | CONFIGURATION OF SECURITY POLICY FILTERS*					
AC-4 (12)	*INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS*					
AC-4 (13)	*INFORMATION FLOW ENFORCEMENT | DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS*					
AC-4 (14)	*INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTER CONSTRAINTS*					
AC-4 (15)	*INFORMATION FLOW ENFORCEMENT | DETECTION OF UNSANCTIONED INFORMATION*					
AC-4 (16)	*INFORMATION FLOW ENFORCEMENT | INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS*	x	Incorporated into AC-4.			
AC-4 (17)	*INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION*					
AC-4 (18)	*INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING*					
AC-4 (19)	*INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA*					
AC-4 (20)	*INFORMATION FLOW ENFORCEMENT | CLASSIFIED INFORMATION*					
AC-4 (21)	*INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS*					
AC-4 (22)	*INFORMATION FLOW ENFORCEMENT | ACCESS ONLY*					
AC-5	**Separation of Duties**				x	x
AC-6	**Least Privilege**				x	x
AC-6 (1)	*LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*				x	x
AC-6 (2)	*LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*				x	x
AC-6 (3)	*LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*					x
AC-6 (4)	*LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*					
AC-6 (5)	*LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*				x	x
AC-6 (6)	*LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*					
AC-6 (7)	*LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*					
AC-6 (8)	*LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*					

Deleted: *MANDATORY*

Deleted: *ROLE-BASED*

Deleted: *CONTROL*

Deleted: *REVOCATION OF ACCESS AUTHORIZATIONS*

Deleted: *NETWORK*

Deleted: *SECURITY-RELATED FUNCTIONS*

Deleted: *CONDITION / OPERATIONAL CHANGES*

Deleted: *DATA*

Deleted: *TYPES*

Deleted: *ON DATA STRUCTURES AND CONTENT*

Deleted: *PROTECTION*

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-6 (9)	*LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*				X	X
AC-6 (10)	*LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*				X	X
AC-7	**Unsuccessful Logon Attempts**			X	X	X
AC-7 (1)	*UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK*	X	Incorporated into AC-7.			
AC-7 (2)	*UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE*					
AC-8	**System Use Notification**			X	X	X
AC-9	**Previous Logon (Access) Notification**					
AC-9 (1)	*PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS*					
AC-9 (2)	*PREVIOUS LOGON NOTIFICATION | SUCCESSFUL / UNSUCCESSFUL LOGONS*					
AC-9 (3)	*PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES*					
AC-9 (4)	*PREVIOUS LOGON NOTIFICATION | ADDITIONAL LOGON INFORMATION*					
AC-10	**Concurrent Session Control**					X
AC-11	**Session Lock**				X	X
AC-11 (1)	*SESSION LOCK | PATTERN-HIDING DISPLAYS*				X	X
AC-12	**Session Termination**	X	Incorporated into SC-10.			
AC-13	**Supervision and Review — Access Control**	X	Incorporated into AC-2 and AU-6.			
AC-14	**Permitted Actions without Identification or Authentication**			X	X	X
AC-14 (1)	*PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES*	X	Incorporated into AC-14.			
AC-15	**Automated Marking**	X	Incorporated into MP-3.			
AC-16	**Security Attributes**					
AC-16 (1)	*SECURITY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION*					
AC-16 (2)	*SECURITY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS*					
AC-16 (3)	*SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM*					
AC-16 (4)	*SECURITY ATTRIBUTES | ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS*					
AC-16 (5)	*SECURITY ATTRIBUTES | ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES*					
AC-16 (6)	*SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION*					
AC-16 (7)	*SECURITY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION*					
AC-16 (8)	*SECURITY ATTRIBUTES | ASSOCIATION TECHNIQUES / TECHNOLOGIES*					
AC-16 (9)	*SECURITY ATTRIBUTES | ATTRIBUTE REASSIGNMENT*					
AC-16 (10)	*SECURITY ATTRIBUTES | ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS*					
AC-17	**Remote Access**			X	X	X
AC-17 (1)	*REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*				X	X
AC-17 (2)	*REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*				X	X
AC-17 (3)	*REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*				X	X
AC-17 (4)	*REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*				X	X
AC-17 (5)	*REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS*	X	Incorporated into AC-17.			
AC-17 (6)	*REMOTE ACCESS | PROTECTION OF INFORMATION*					
AC-17 (7)	*REMOTE ACCESS | ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS*	X	Incorporated into AC-3.			

Deleted: Login

Deleted: *LOGIN*

Deleted: W

Deleted: *LOGIN*

Deleted: W

Deleted: Incorporated into AC-11.

Deleted: W

Deleted: W

Deleted: W

Deleted: W

Deleted: AC-16 (11)

Deleted: W

Deleted: W

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-17 (8)	*REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS*	X	Incorporated into CM-7.			
AC-17 (9)	*REMOTE ACCESS | DISCONNECT / DISABLE ACCESS*					
AC-18	**Wireless Access**			X	X	X
AC-18 (1)	*WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*				X	X
AC-18 (2)	*WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS*	X	Incorporated into SI-4.			
AC-18 (3)	*WIRELESS ACCESS | DISABLE WIRELESS NETWORKING*					
AC-18 (4)	*WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*					X
AC-18 (5)	*WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS*					X
AC-19	**Access Control for Mobile Devices**			X	X	X
AC-19 (1)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE / PORTABLE STORAGE DEVICES*	X	Incorporated into MP-7.			
AC-19 (2)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES*	X	Incorporated into MP-7.			
AC-19 (3)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER*	X	Incorporated into MP-7.			
AC-19 (4)	*ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION*					
AC-19 (5)	*ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION*				X	X
AC-20	**Use of External Information Systems**			X	X	X
AC-20 (1)	*USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE*				X	X
AC-20 (2)	*USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES*				X	X
AC-20 (3)	*USE OF EXTERNAL INFORMATION SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES*					
AC-20 (4)	*USE OF EXTERNAL INFORMATION SYSTEMS | NETWORK ACCESSIBLE STORAGE DEVICES*					
AC-21	**Information Sharing**				X	X
AC-21 (1)	*INFORMATION SHARING | AUTOMATED DECISION SUPPORT*					
AC-21 (2)	*INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL*					
AC-22	**Publicly Accessible Content**			X	X	X
AC-23	**Data Mining Protection**					
AC-24	**Access Control Decisions**					
AC-24 (1)	*ACCESS CONTROL DECISIONS | TRANSMIT ACCESS AUTHORIZATION INFORMATION*					
AC-24 (2)	*ACCESS CONTROL DECISIONS | NO USER OR PROCESS IDENTITY*					
AC-25	**Reference Monitor**		X			

Deleted: W
Deleted: W
Deleted: AC-18
Deleted: *CONFINE WIRELESS COMMUNICATIONS*
Deleted: W
Deleted: *REMOVABLE MEDIA*
Deleted: W
Deleted: *REMOVABLE MEDIA*
Deleted: *REMOVABLE MEDIA*
Deleted: W
Deleted: AC-19 (5) ...
Deleted: 6
Deleted: *DISK*
Deleted: AC-19 (7) ...
Deleted: *MEDIA*
Deleted: *PERSONALLY*
Deleted: *INFORMATION*
Deleted: Collaboration and
Deleted: *COLLABORATION AND*
Deleted: *COLLABORATION AND*
Deleted: Function
Deleted: A

TABLE D-4: SUMMARY — AWARENESS AND TRAINING CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AT-1	**Security Awareness and Training Policy and Procedures**			x	x	x
AT-2	**Security Awareness Training**			x	x	x
AT-2 (1)	*SECURITY AWARENESS | PRACTICAL EXERCISES*					
AT-2 (2)	*SECURITY AWARENESS | INSIDER THREAT*				x	x
AT-3	**Role-Based Security Training**			x	x	x
AT-3 (1)	*SECURITY TRAINING | ENVIRONMENTAL CONTROLS*					
AT-3 (2)	*SECURITY TRAINING | PHYSICAL SECURITY CONTROLS*					
AT-3 (3)	*SECURITY TRAINING | PRACTICAL EXERCISES*					
AT-3 (4)	*SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR*					
AT-4	**Security Training Records**			x	x	x
AT-5	**Contacts with Security Groups and Associations**	x	Incorporated into PM-15.			

Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A

TABLE D-5: SUMMARY — AUDIT AND ACCOUNTABILITY CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AU-1	**Audit and Accountability Policy and Procedures**		x	x	x	x
AU-2	**Audit Events**			x	x	x
AU-2 (1)	*AUDIT EVENTS | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES*	x	Incorporated into AU-12.			
AU-2 (2)	*AUDIT EVENTS | SELECTION OF AUDIT EVENTS BY COMPONENT*	x	Incorporated into AU-12.			
AU-2 (3)	*AUDIT EVENTS | REVIEWS AND UPDATES*				x	x
AU-2 (4)	*AUDIT EVENTS | PRIVILEGED FUNCTIONS*	x	Incorporated into AC-6.			
AU-3	**Content of Audit Records**			x	x	x
AU-3 (1)	*CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*				x	x
AU-3 (2)	*CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*					x
AU-4	**Audit Storage Capacity**			x	x	x
AU-4 (1)	*AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*					
AU-5	**Response to Audit Processing Failures**			x	x	x
AU-5 (1)	*RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY*					x
AU-5 (2)	*RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS*					x
AU-5 (3)	*RESPONSE TO AUDIT PROCESSING FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS*					
AU-5 (4)	*RESPONSE TO AUDIT PROCESSING FAILURES | SHUTDOWN ON FAILURE*					
AU-6	**Audit Review, Analysis, and Reporting**		x	x	x	x
AU-6 (1)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION*		x		x	x
AU-6 (2)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS*	x	Incorporated into SI-4.			
AU-6 (3)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES*		x		x	x
AU-6 (4)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS*		x			
AU-6 (5)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES*		x			x
AU-6 (6)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING*		x			x
AU-6 (7)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS*		x			
AU-6 (8)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS*		x			
AU-6 (9)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES*		x			
AU-6 (10)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT*		x			
AU-7	**Audit Reduction and Report Generation**		x		x	x
AU-7 (1)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*		x		x	x
AU-7 (2)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH*					
AU-8	**Time Stamps**			x	x	x
AU-8 (1)	*TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*				x	x
AU-8 (2)	*TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE*					

Deleted: A
Deleted: Auditable
Deleted: *AUDITABLE*
Deleted: W
Deleted: *AUDITABLE*
Deleted: W
Deleted: *AUDITABLE*
Deleted: *AUDITABLE*
Deleted: x
Deleted: A
Deleted: A
Deleted: W
Deleted: A
Deleted: A
Deleted: W
Deleted: Incorporated into AU-6.
Deleted: A
Deleted: A
Deleted: x
Deleted: x
Deleted: *INPUT*
Deleted: *NON-TECHNICAL*
Deleted: A
Deleted: A
Deleted: *SORTING*

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AU-9	**Protection of Audit Information**			x	x	x
AU-9 (1)	*PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE* MEDIA					
AU-9 (2)	*PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*					x
AU-9 (3)	*PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION*					x
AU-9 (4)	*PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*				x	x
AU-9 (5)	*PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION*					
AU-9 (6)	*PROTECTION OF AUDIT INFORMATION | READ ONLY ACCESS*					
AU-10	**Non-repudiation**		x			
AU-10 (1)	*NON-REPUDIATION | ASSOCIATION OF IDENTITIES*		x			
AU-10 (2)	*NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY*		x			
AU-10 (3)	*NON-REPUDIATION | CHAIN OF CUSTODY*		x			
AU-10 (4)	*NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY*		x			
AU-10 (5)	*NON-REPUDIATION | DIGITAL SIGNATURES*	x	Incorporated into SI-7.			
AU-11	**Audit Record Retention**			x	x	x
AU-12	**Audit Generation**			x	x	x
AU-12 (1)	*AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL*					x
AU-12 (2)	*AUDIT GENERATION | STANDARDIZED FORMATS*					
AU-12 (3)	*AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS*					x
AU-13	**Monitoring for Information Disclosure**		x			
AU-13 (1)	*MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS*		x			
AU-13 (2)	*MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES*		x			
AU-14	**Session Audit**		x			
AU-14 (1)	*SESSION AUDIT | SYSTEM START-UP*		x			
AU-14 (2)	*SESSION AUDIT | REMOTE VIEWING / LISTENING*		x			
AU-15	**Alternate Audit Capability**					
AU-16	**Cross-Organizational Auditing**					
AU-16 (1)	*CROSS-ORGANIZATIONAL AUDITING | IDENTITY PRESERVATION*					
AU-16 (2)	*CROSS-ORGANIZATIONAL AUDITING | SHARING OF AUDIT INFORMATION*					

Deleted: A
Deleted: x
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: W
Deleted: A
Deleted: A
Deleted: A

TABLE D-6: SUMMARY — SECURITY ASSESSMENT AND AUTHORIZATION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CA-1	**Security Assessment and Authorization Policies and Procedures**		x	x	x	x
CA-2	**Security Assessments**		x	x	x	x
CA-2 (1)	*SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*		x		x	x
CA-2 (2)	*SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS*		x			x
CA-2 (3)	*SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS*		x			
CA-3	**System Interconnections**		x	x	x	x
CA-3 (1)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*					
CA-3 (2)	*SYSTEM INTERCONNECTIONS | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*					
CA-3 (3)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS*					
CA-3 (4)	*SYSTEM INTERCONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS*					
CA-3 (5)	*SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL NETWORK CONNECTIONS*				x	x
CA-4	**Security Certification**	x	Incorporated into CA-2.			
CA-5	**Plan of Action and Milestones**		x	x	x	x
CA-5 (1)	*PLAN OF ACTION AND MILESTONES | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*		x			
CA-6	**Security Authorization**		x	x	x	x
CA-7	**Continuous Monitoring**		x	x	x	x
CA-7 (1)	*CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT*		x		x	x
CA-7 (2)	*CONTINUOUS MONITORING | TYPES OF ASSESSMENTS*	x	Incorporated into CA-2.			
CA-7 (3)	*CONTINUOUS MONITORING | TREND ANALYSES*		x			
CA-8	**Penetration Testing**		x			x
CA-8 (1)	*PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM*		x			
CA-8 (2)	*PENETRATION TESTING | RED TEAM EXERCISES*		x			
CA-9	**Internal System Connections**		x	x	x	x
CA-9 (1)	*INTERNAL SYSTEM CONNECTIONS | SECURITY COMPLIANCE CHECKS*		x			

Deleted: A
Deleted: A
Deleted: A
Deleted: TYPES OF
Deleted: A
Deleted: A
Deleted: Information
Deleted: Connections
Deleted: A
Deleted: INFORMATION
Deleted: CONNECTIONS
Deleted: INFORMATION
Deleted: CONNECTIONS
Deleted: CONNECTION
Deleted: 3
Deleted: INFORMATION
Deleted: CONNECTIONS | PROHIBIT
Deleted: W
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: W

TABLE D-7: SUMMARY — CONFIGURATION MANAGEMENT CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CM-1	**Configuration Management Policy and Procedures**		x	x	x	x
CM-2	**Baseline Configuration**		x	x	x	x
CM-2 (1)	*BASELINE CONFIGURATION | REVIEWS AND UPDATES*		x		x	x
CM-2 (2)	*BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*		x			x
CM-2 (3)	*BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*		x		x	x
CM-2 (4)	*BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE*	x	Incorporated into CM-7.			
CM-2 (5)	*BASELINE CONFIGURATION | AUTHORIZED SOFTWARE*	x	Incorporated into CM-7.			
CM-2 (6)	*BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS*		x			
CM-2 (7)	*BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*		x		x	x
CM-3	**Configuration Change Control**		x		x	x
CM-3 (1)	*CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES*		x			x
CM-3 (2)	*CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*	x	Incorporated into CM-4.			
CM-3 (3)	*CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION*					
CM-3 (4)	*CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE*					
CM-3 (5)	*CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE*					
CM-3 (6)	*CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT*					
CM-4	**Security Impact Analysis**		x	x	x	x
CM-4 (1)	*SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS*		x			x
CM-4 (2)	*SECURITY IMPACT ANALYSIS | VERIFICATION OF SECURITY FUNCTIONS*		x			
CM-4 (3)	*SECURITY IMPACT ANALYSIS | TEST / VALIDATE / DOCUMENT CHANGES*		x		x	x
CM-5	**Access Restrictions for Change**				x	x
CM-5 (1)	*ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING*					x
CM-5 (2)	*ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES*					x
CM-5 (3)	*ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS*					x
CM-5 (4)	*ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION*					
CM-5 (5)	*ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES*					
CM-5 (6)	*ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES*					
CM-5 (7)	*ACCESS RESTRICTIONS FOR CHANGE | AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS*	x	Incorporated into SI-7.			
CM-6	**Configuration Settings**			x	x	x
CM-6 (1)	*CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION*					x
CM-6 (2)	*CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES*					x
CM-6 (3)	*CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION*	x	Incorporated into SI-7.			
CM-6 (4)	*CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION*	x	Incorporated into CM-4.			
CM-7	**Least Functionality**			x	x	x

Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: W
Deleted: W
Deleted: A
Deleted: x
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: *AUDIT*
Deleted: *TWO-PERSON RULE*
Deleted: W
Deleted: W
Deleted: W
Deleted: CA-2 and CA-7

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CM-7 (1)	*LEAST FUNCTIONALITY | PERIODIC REVIEW*				x	x
CM-7 (2)	*LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION*				x	x
CM-7 (3)	*LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE*					
CM-7 (4)	*LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING*				x	
CM-7 (5)	*LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING*					x
CM-8	**Information System Component Inventory**		x	x	x	x
CM-8 (1)	*INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*		x		x	x
CM-8 (2)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*		x			x
CM-8 (3)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*		x		x	x
CM-8 (4)	*INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION*		x			x
CM-8 (5)	*INFORMATION SYSTEM COMPONENT INVENTORY | ALL COMPONENTS WITHIN AUTHORIZATION BOUNDARY*		x		x	x
CM-8 (6)	*INFORMATION SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS*		x			
CM-8 (7)	*INFORMATION SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY*		x			
CM-8 (8)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING*		x			
CM-8 (9)	*INFORMATION SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS*		x			
CM-9	**Configuration Management Plan**				x	x
CM-9 (1)	*CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY*					
CM-10	**Software Usage Restrictions**			x	x	x
CM-10 (1)	*SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE*					
CM-11	**User-Installed Software**			x	x	x
CM-11 (1)	*USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS*					
CM-11 (2)	*USER-INSTALLED SOFTWARE | PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS*					

Deleted: A

Deleted: A

Deleted: A

Deleted: A

Deleted: *PROPERTY*

Deleted: A

Deleted: A

Deleted: *AUTOMATED*

TABLE D-8: SUMMARY — CONTINGENCY PLANNING CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		X	X	X	X
CP-2	**Contingency Plan**			X	X	X
CP-2 (1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				X	X
CP-2 (2)	*CONTINGENCY PLAN | CAPACITY PLANNING*					X
CP-2 (3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*				X	X
CP-2 (4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*					X
CP-2 (5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					X
CP-2 (6)	*CONTINGENCY PLAN | ALTERNATE PROCESSING / STORAGE SITE*					
CP-2 (7)	*CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS*					
CP-2 (8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*				X	X
CP-3	**Contingency Training**		X	X	X	X
CP-3 (1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*		X			X
CP-3 (2)	*CONTINGENCY TRAINING | AUTOMATED TRAINING ENVIRONMENTS*		X			
CP-4	**Contingency Plan Testing**		X	X	X	X
CP-4 (1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		X		X	X
CP-4 (2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*		X			X
CP-4 (3)	*CONTINGENCY PLAN TESTING | AUTOMATED TESTING*		X			
CP-4 (4)	*CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION*		X			
CP-5	**Contingency Plan Update**	X	Incorporated into CP-2.			
CP-6	**Alternate Storage Site**				X	X
CP-6 (1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*				X	X
CP-6 (2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*					X
CP-6 (3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*				X	X
CP-7	**Alternate Processing Site**				X	X
CP-7 (1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*				X	X
CP-7 (2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*				X	X
CP-7 (3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*				X	X
CP-7 (4)	*ALTERNATE PROCESSING SITE | PREPARATION FOR USE*					X
CP-7 (5)	*ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*	X	Incorporated into CP-7.			
CP-7 (6)	*ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE*					
CP-8	**Telecommunications Services**				X	X
CP-8 (1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*				X	X
CP-8 (2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*				X	X
CP-8 (3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*					X
CP-8 (4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*					X
CP-8 (5)	*TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING*					
CP-9	**Information System Backup**			X	X	X
CP-9 (1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*				X	X

Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: x
Deleted: W
Deleted: *CONFIGURATION*
Deleted: W

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-9 (2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*					x
CP-9 (3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*					x
CP-9 (4)	*INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*	x	Incorporated into CP-9.			
CP-9 (5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*					x
CP-9 (6)	*INFORMATION SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM*					
CP-9 (7)	*INFORMATION SYSTEM BACKUP | DUAL AUTHORIZATION*					
CP-10	**Information System Recovery and Reconstitution**			x	x	x
CP-10 (1)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*	x	Incorporated into CP-4.			
CP-10 (2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*				x	x
CP-10 (3)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*	x	Addressed by tailoring procedures.			
CP-10 (4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*					x
CP-10 (5)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*	x	Incorporated into SI-13.			
CP-10 (6)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION*					
CP-11	**Alternate Communications Protocols**					
CP-12	**Safe Mode**		x			
CP-13	**Alternative Security Mechanisms**					

Deleted: W

Deleted: *TWO-PERSON RULE*

Deleted: W

Deleted: x

Deleted: x

Deleted: CP-11

Moved down [20]: *PREDICTABLE FAILURE PREVENTION \| TRANSFERRING COMPONENT RESPONSIBILITIES*

Moved down [21]: *PREDICTABLE FAILURE PREVENTION \| TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*

Moved down [22]: *PREDICTABLE FAILURE PREVENTION \| MANUAL TRANSFER BETWEEN COMPONENTS*

Moved down [23]: *PREDICTABLE FAILURE PREVENTION \| STANDBY COMPONENT INSTALLATION / NOTIFICATION*

Deleted: 12

Deleted: 13

Deleted: A

TABLE D-9: SUMMARY — IDENTIFICATION AND AUTHENTICATION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
IA-1	**Identification and Authentication Policy and Procedures**		x	x	x	x
IA-2	**Identification and Authentication (Organizational Users)**			x	x	x
IA-2 (1)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*			x	x	x
IA-2 (2)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*				x	x
IA-2 (3)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*				x	x
IA-2 (4)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS*					x
IA-2 (5)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | GROUP AUTHENTICATION*					
IA-2 (6)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE*					
IA-2 (7)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE*					
IA-2 (8)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*				x	x
IA-2 (9)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT*					x
IA-2 (10)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | SINGLE SIGN-ON*					
IA-2 (11)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE*				x	x
IA-2 (12)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE*				x	x
IA-2 (13)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS*			x	x	x
IA-3	**Device Identification and Authentication**				x	x
IA-3 (1)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*					
IA-3 (2)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION*	x	Incorporated into IA-3 (1).			
IA-3 (3)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION*					
IA-3 (4)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION*					
IA-4	**Identifier Management**			x	x	x
IA-4 (1)	*IDENTIFIER MANAGEMENT | PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS*					
IA-4 (2)	*IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION*					
IA-4 (3)	*IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION*					
IA-4 (4)	*IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS*					
IA-4 (5)	*IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT*					
IA-4 (6)	*IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT*					
IA-4 (7)	*IDENTIFIER MANAGEMENT | IN PERSON REGISTRATION*					
IA-5	**Authenticator Management**			x	x	x

Deleted: A

Deleted: | *INDIVIDUAL AND*

Deleted: *AUTHENTICATORS*

Deleted: Device-to-

Deleted: *DEVICE-TO-*

Deleted: *DEVICE-TO-*

Deleted: W

Deleted: .

Deleted: *DEVICE-TO-*

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
IA-5 (1)	*AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*			x	x	x
IA-5 (2)	*AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*				x	x
IA-5 (3)	*AUTHENTICATOR MANAGEMENT | IN PERSON OR TRUSTED THIRD-PARTY REGISTRATION*				x	x
IA-5 (4)	*AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION*					
IA-5 (5)	*AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY*					
IA-5 (6)	*AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS*					
IA-5 (7)	*AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS*					
IA-5 (8)	*AUTHENTICATOR MANAGEMENT | MULTIPLE INFORMATION SYSTEM ACCOUNTS*					
IA-5 (9)	*AUTHENTICATOR MANAGEMENT | CROSS-ORGANIZATION CREDENTIAL MANAGEMENT*					
IA-5 (10)	*AUTHENTICATOR MANAGEMENT | DYNAMIC CREDENTIAL ASSOCIATION*					
IA-5 (11)	*AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION*			x	x	x
IA-5 (12)	*AUTHENTICATOR MANAGEMENT | BIOMETRIC AUTHENTICATION*					
IA-5 (13)	*AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS*					
IA-5 (14)	*AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES*					
IA-5 (15)	*AUTHENTICATOR MANAGEMENT | FICAM-APPROVED PRODUCTS AND SERVICES*					
IA-6	**Authenticator Feedback**			x	x	x
IA-7	**Cryptographic Module Authentication**			x	x	x
IA-8	**Identification and Authentication (Non-Organizational Users)**			x	x	x
IA-8 (1)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*			x	x	x
IA-8 (2)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*			x	x	x
IA-8 (3)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS*			x	x	x
IA-8 (4)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-ISSUED PROFILES*			x	x	x
IA-8 (5)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV-I CREDENTIALS*					
IA-9	**Service Identification and Authentication**					
IA-9 (1)	*SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE*					
IA-9 (2)	*SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS*					
IA-10	**Adaptive Identification and Authentication**					
IA-11	**Re-authentication**					

Deleted: *TOOLS*

Deleted: *AUTHENTICATOR*

Deleted: IA-10 ...

Deleted: 11

Deleted: 12

Deleted: Reauthentication

TABLE D-10: SUMMARY — INCIDENT RESPONSE CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
IR-1	**Incident Response Policy and Procedures**			x	x	x
IR-2	**Incident Response Training**			x	x	x
IR-2 (1)	*INCIDENT RESPONSE TRAINING | SIMULATED EVENTS*					x
IR-2 (2)	*INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS*					x
IR-3	**Incident Response Testing**				x	x
IR-3 (1)	*INCIDENT RESPONSE TESTING | AUTOMATED TESTING*					
IR-3 (2)	*INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS*				x	x
IR-4	**Incident Handling**			x	x	x
IR-4 (1)	*INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES*				x	x
IR-4 (2)	*INCIDENT HANDLING | DYNAMIC RECONFIGURATION*					
IR-4 (3)	*INCIDENT HANDLING | CONTINUITY OF OPERATIONS*					
IR-4 (4)	*INCIDENT HANDLING | INFORMATION CORRELATION*					x
IR-4 (5)	*INCIDENT HANDLING | AUTOMATIC DISABLING OF INFORMATION SYSTEM*					
IR-4 (6)	*INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES*					
IR-4 (7)	*INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION*					
IR-4 (8)	*INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS*					
IR-4 (9)	*INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY*					
IR-4 (10)	*INCIDENT HANDLING | SUPPLY CHAIN COORDINATION*					
IR-5	**Incident Monitoring**			x	x	x
IR-5 (1)	*INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS*					x
IR-6	**Incident Reporting**			x	x	x
IR-6 (1)	*INCIDENT REPORTING | AUTOMATED REPORTING*				x	x
IR-6 (2)	*INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS*					
IR-6 (3)	*INCIDENT REPORTING | COORDINATION WITH SUPPLY CHAIN*					
IR-7	**Incident Response Assistance**			x	x	x
IR-7 (1)	*INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT*				x	x
IR-7 (2)	*INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS*					
IR-8	**Incident Response Plan**			x	x	x
IR-9	**Information Spillage Response**					
IR-9 (1)	*INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL*					
IR-9 (2)	*INFORMATION SPILLAGE RESPONSE | TRAINING*					
IR-9 (3)	*INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS*					
IR-9 (4)	*INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL*					
IR-10	**Integrated Information Security Cell**					

Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: x
Deleted: A
Deleted: A
Deleted: A

TABLE D-11: SUMMARY — MAINTENANCE CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
MA-1	**System Maintenance Policy and Procedures**			x	x	x
MA-2	**Controlled Maintenance**			x	x	x
MA-2 (1)	*CONTROLLED MAINTENANCE | RECORD CONTENT*	x	Incorporated into MA-2.			
MA-2 (2)	*CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES*					x
MA-3	**Maintenance Tools**				x	x
MA-3 (1)	*MAINTENANCE TOOLS | INSPECT TOOLS*				x	x
MA-3 (2)	*MAINTENANCE TOOLS | INSPECT MEDIA*				x	x
MA-3 (3)	*MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*					x
MA-3 (4)	*MAINTENANCE TOOLS | RESTRICTED TOOL USE*					
MA-4	**Nonlocal Maintenance**			x	x	x
MA-4 (1)	*NONLOCAL MAINTENANCE | AUDITING AND REVIEW*					
MA-4 (2)	*NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE*				x	x
MA-4 (3)	*NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION*					x
MA-4 (4)	*NONLOCAL MAINTENANCE | AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS*					
MA-4 (5)	*NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS*					
MA-4 (6)	*NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION*					
MA-4 (7)	*NONLOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION*					
MA-5	**Maintenance Personnel**			x	x	x
MA-5 (1)	*MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS*					x
MA-5 (2)	*MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS*					
MA-5 (3)	*MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS*					
MA-5 (4)	*MAINTENANCE PERSONNEL | FOREIGN NATIONALS*					
MA-5 (5)	*MAINTENANCE PERSONNEL | NON SYSTEM-RELATED MAINTENANCE*					
MA-6	**Timely Maintenance**				x	x
MA-6 (1)	*TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE*					
MA-6 (2)	*TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE*					
MA-6 (3)	*TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE*					

Deleted: A

Deleted: W

Deleted: AUTOMATED

Deleted: Non-Local

Deleted: NON-LOCAL

Deleted: x

Deleted: x

Deleted: NON-LOCAL

Deleted: NON-LOCAL

Deleted: NON-LOCAL

Deleted: NON-LOCAL

Deleted: NON-LOCAL

Deleted: NON-LOCAL

Deleted: NON-LOCAL

TABLE D-12: SUMMARY — MEDIA PROTECTION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
MP-1	**Media Protection Policy and Procedures**		x	x	x	x
MP-2	**Media Access**			x	x	x
MP-2 (1)	*MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS*	x	Incorporated into MP-4 (2).			
MP-2 (2)	*MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION*	x	Incorporated into SC-28 (1).			
MP-3	**Media Marking**				x	x
MP-4	**Media Storage**				x	x
MP-4 (1)	*MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION*	x	Incorporated into SC-28 (1).			
MP-4 (2)	*MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS*					
MP-5	**Media Transport**				x	x
MP-5 (1)	*MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS*	x	Incorporated into MP-5.			
MP-5 (2)	*MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES*	x	Incorporated into MP-5.			
MP-5 (3)	*MEDIA TRANSPORT | CUSTODIANS*					
MP-5 (4)	*MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*				x	x
MP-6	**Media Sanitization**			x	x	x
MP-6 (1)	*MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY*					x
MP-6 (2)	*MEDIA SANITIZATION | EQUIPMENT TESTING*					x
MP-6 (3)	*MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES*					x
MP-6 (4)	*MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION*	x	Incorporated into MP-6.			
MP-6 (5)	*MEDIA SANITIZATION | CLASSIFIED INFORMATION*	x	Incorporated into MP-6.			
MP-6 (6)	*MEDIA SANITIZATION | MEDIA DESTRUCTION*	x	Incorporated into MP-6.			
MP-6 (7)	*MEDIA SANITIZATION | DUAL AUTHORIZATION*					
MP-6 (8)	*MEDIA SANITIZATION | REMOTE PURGING / WIPING OF INFORMATION*					
MP-7	**Media Use**			x	x	x
MP-7 (1)	*MEDIA USE | PROHIBIT USE WITHOUT OWNER*				x	x
MP-7 (2)	*MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA*					
MP-8	**Media Downgrading**					
MP-8 (1)	*MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS*					
MP-8 (2)	*MEDIA DOWNGRADING | EQUIPMENT TESTING*					
MP-8 (3)	*MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION*					
MP-8 (4)	*MEDIA DOWNGRADING | CLASSIFIED INFORMATION*					

Deleted: A

Deleted: x

Deleted: OFF-LINE STORAGE

Deleted: W

Deleted: W

Deleted: x

Deleted: TRACKING / DOCUMENTING / VERIFYING

Deleted: NON-DESTRUCTIVE

Deleted: W

Deleted: W

Deleted: W

Deleted: TWO-PERSON RULE

Deleted: ORGANIZATIONAL RESTRICTIONS

Deleted: PROHIBITION OF

Deleted: WITHOUT OWNER

Deleted: x

Deleted: x

Deleted: TRACKING / DOCUMENTING

TABLE D-13: SUMMARY — PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PE-1	**Physical and Environmental Protection Policy and Procedures**		X	X	X	X
PE-2	**Physical Access Authorizations**			X	X	X
PE-2 (1)	*PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION / ROLE*					
PE-2 (2)	*PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION*					
PE-2 (3)	*PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS*					
PE-3	**Physical Access Control**			X	X	X
PE-3 (1)	*PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*					X
PE-3 (2)	*PHYSICAL ACCESS CONTROL | FACILITY / INFORMATION SYSTEM BOUNDARIES*					
PE-3 (3)	*PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS / ALARMS / MONITORING*					
PE-3 (4)	*PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS*					
PE-3 (5)	*PHYSICAL ACCESS CONTROL | TAMPER PROTECTION*					
PE-3 (6)	*PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING*					
PE-4	**Access Control for Transmission Medium**				X	X
PE-5	**Access Control for Output Devices**				X	X
PE-5 (1)	*ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS*					
PE-5 (2)	*ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY*					
PE-5 (3)	*ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES*					
PE-6	**Monitoring Physical Access**		X	X	X	X
PE-6 (1)	*MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*		X		X	X
PE-6 (2)	*MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION / RESPONSES*		X			
PE-6 (3)	*MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE*		X			
PE-6 (4)	*MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*		X			X
PE-7	**Visitor Control**	X	Incorporated into PE-2 and PE-3.			
PE-8	**Visitor Access Records**		X	X	X	X
PE-8 (1)	*VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW*					X
PE-8 (2)	*VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS*	X	Incorporated into PE-2.			
PE-9	**Power Equipment and Cabling**				X	X
PE-9 (1)	*POWER EQUIPMENT AND CABLING | REDUNDANT CABLING*					
PE-9 (2)	*POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS*					
PE-10	**Emergency Shutoff**				X	X
PE-10 (1)	*EMERGENCY SHUTOFF | ACCIDENTAL / UNAUTHORIZED ACTIVATION*	X	Incorporated into PE-10.			
PE-11	**Emergency Power**				X	X
PE-11 (1)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*					X
PE-11 (2)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED*					

Deleted: A
Deleted: 1
Deleted: AUTOMATED
Deleted: CONTROL /
Deleted: LINKAGE
Deleted: A
Deleted: A
Deleted: A
Deleted: x
Deleted: 3
Deleted: VIDEO SURVEILLANCE
Deleted: A
Deleted: W
Deleted: A
Deleted: W
Deleted: W

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PE-12	**Emergency Lighting**			x	x	x
PE-12 (1)	*EMERGENCY LIGHTING | ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					
PE-13	**Fire Protection**			x	x	x
PE-13 (1)	*FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*					x
PE-13 (2)	*FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*					x
PE-13 (3)	*FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*				x	x
PE-13 (4)	*FIRE PROTECTION | INSPECTIONS*					
PE-14	**Temperature and Humidity Controls**			x	x	x
PE-14 (1)	*TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS*					
PE-14 (2)	*TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS*					
PE-15	**Water Damage Protection**			x	x	x
PE-15 (1)	*WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*					x
PE-16	**Delivery and Removal**			x	x	x
PE-17	**Alternate Work Site**				x	x
PE-18	**Location of Information System Components**					x
PE-18 (1)	*LOCATION OF INFORMATION SYSTEM COMPONENTS | FACILITY SITE*					
PE-19	**Information Leakage**					
PE-19 (1)	*INFORMATION LEAKAGE | NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES*					

Deleted: x

Deleted: x

Deleted: x

Deleted: x

Deleted: x

Deleted: PE-20 ...

TABLE D-14: SUMMARY — PLANNING CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PL-1	**Security Planning Policy and Procedures**		x	x	x	x
PL-2	**System Security Plan**		x	x	x	x
PL-2 (1)	*SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS*	x	Incorporated into PL-7.			
PL-2 (2)	*SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE*	x	Incorporated into PL-8.			
PL-2 (3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*		x		x	x
PL-3	**System Security Plan Update**	x	Incorporated into PL-2.			
PL-4	**Rules of Behavior**		x	x	x	x
PL-4 (1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*		x		x	x
PL-5	**Privacy Impact Assessment**	x	Incorporated into Appendix J, AR-2.			
PL-6	**Security-Related Activity Planning**	x	Incorporated into PL-2.			
PL-7	**Security Concept of Operations**					
PL-8	**Information Security Architecture**		x		x	x
PL-8 (1)	*INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH*		x			
PL-8 (2)	*INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY*		x			
PL-9	**Central Management**		x			

Deleted: A
Deleted: A
Deleted: W
Deleted: W
Deleted: A
Deleted: W
Deleted: A
Deleted: A
Deleted: W
Deleted: W

TABLE D-15: SUMMARY — PERSONNEL SECURITY CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PS-1	**Personnel Security Policy and Procedures**		x	x	x	x
PS-2	**Position Risk Designation**			x	x	x
PS-3	**Personnel Screening**			x	x	x
PS-3 (1)	*PERSONNEL SCREENING | CLASSIFIED INFORMATION*					
PS-3 (2)	*PERSONNEL SCREENING | FORMAL INDOCTRINATION*					
PS-3 (3)	*PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES*					
PS-4	**Personnel Termination**			x	x	x
PS-4 (1)	*PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS*					
PS-4 (2)	*PERSONNEL TERMINATION | AUTOMATED NOTIFICATION*					x
PS-5	**Personnel Transfer**			x	x	x
PS-6	**Access Agreements**		x	x	x	x
PS-6 (1)	*ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION*	x	Incorporated into PS-3.			
PS-6 (2)	*ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION*		x			
PS-6 (3)	*ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS*		x			
PS-7	**Third-Party Personnel Security**		x	x	x	x
PS-8	**Personnel Sanctions**			x	x	x

Deleted: A

Deleted: Categorization

Deleted: PS-3 (3) ...

Deleted: 4

Deleted: x

Deleted: A

Deleted: W

Deleted: A

Deleted: 7

Moved down [18]: Third-Party Personnel Security

Deleted: A

Deleted: x

Deleted: x

Deleted: x

Moved (insertion) [18]

Deleted: (1)

Deleted: *THIRD-PARTY PERSONNEL SECURITY \| NOTIFICATIONS*

Deleted: A

Deleted: PS-8 (1) ...

TABLE D-16: SUMMARY — RISK ASSESSMENT CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
RA-1	**Risk Assessment Policy and Procedures**			x	x	x
RA-2	**Security Categorization**			x	x	x
RA-3	**Risk Assessment**			x	x	x
RA-4	**Risk Assessment Update**	x	Incorporated into RA-3.			
RA-5	**Vulnerability Scanning**			x	x	x
RA-5 (1)	*VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*				x	x
RA-5 (2)	*VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*				x	x
RA-5 (3)	*VULNERABILITY SCANNING | BREADTH /DEPTH OF COVERAGE*					
RA-5 (4)	*VULNERABILITY SCANNING | DISCOVERABLE INFORMATION*					x
RA-5 (5)	*VULNERABILITY SCANNING | PRIVILEGED ACCESS*				x	x
RA-5 (6)	*VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES*					
RA-5 (7)	*VULNERABILITY SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS*	x	Incorporated into CM-8.			
RA-5 (8)	*VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS*					
RA-5 (9)	*VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES*	x	Incorporated into CA-8.			
RA-5 (10)	*VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION*					
RA-6	**Technical Surveillance Countermeasures Survey**					

Deleted: A
Deleted: A
Deleted: W
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: x
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Moved (insertion) [19]

TABLE D-17: SUMMARY — SYSTEM AND SERVICES ACQUISITION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-1	**System and Services Acquisition Policy and Procedures**		X	X	X	X
SA-2	**Allocation of Resources**		X	X	X	X
SA-3	**System Development Life Cycle**		X	X	X	X
SA-4	**Acquisition Process**		X	X	X	X
SA-4 (1)	*ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*		X		X	X
SA-4 (2)	*ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*		X		X	X
SA-4 (3)	*ACQUISITION PROCESS | DEVELOPMENT METHODS / TECHNIQUES / PRACTICES*		X			
SA-4 (4)	*ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS*	X	Incorporated into CM-8 (9).			
SA-4 (5)	*ACQUISITION PROCESS | SYSTEM / COMPONENT / SERVICE CONFIGURATIONS*		X			
SA-4 (6)	*ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS*		X			
SA-4 (7)	*ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES*		X			
SA-4 (8)	*ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN*		X			
SA-4 (9)	*ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*		X		X	X
SA-4 (10)	*ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS*		X	X	X	X
SA-5	**Information System Documentation**		X	X	X	X
SA-5 (1)	*INFORMATION SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*	X	Incorporated into SA-4 (1).			
SA-5 (2)	*INFORMATION SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES*	X	Incorporated into SA-4 (2).			
SA-5 (3)	*INFORMATION SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN*	X	Incorporated into SA-4 (2).			
SA-5 (4)	*INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN*	X	Incorporated into SA-4 (2).			
SA-5 (5)	*INFORMATION SYSTEM DOCUMENTATION | SOURCE CODE*	X	Incorporated into SA-4 (2).			
SA-5 (6)	*INFORMATION SYSTEM DOCUMENTATION | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*	X	Incorporated into SA-4 (9).			
SA-6	**Software Usage Restrictions**	X	Incorporated into CM-10 and SI-7.			
SA-7	**User-Installed Software**	X	Incorporated into CM-11 and SI-7.			
SA-8	**Security Engineering Principles**		X		X	X
SA-9	**External Information System Services**		X	X	X	X
SA-9 (1)	*EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS*		X			
SA-9 (2)	*EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*		X		X	X
SA-9 (3)	*EXTERNAL INFORMATION SYSTEMS | ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS*		X			
SA-9 (4)	*EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS*		X			
SA-9 (5)	*EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION*		X			
SA-10	**Developer Configuration Management**		X		X	X
SA-10 (1)	*DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION*		X			

Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: U.S. GOVERNMENT
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: W
Deleted: W
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: CHAIN OF
Deleted: A
Deleted: x
Deleted: A
Deleted: A
Deleted: A
Deleted: A

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-10 (2)	*DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES*		X			
SA-10 (3)	*DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION*		X			
SA-10 (4)	*DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION*		X			
SA-10 (5)	*DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL*		X			
SA-10 (6)	*DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION*		X			
SA-11	**Developer Security Testing and Evaluation**		X		x	x
SA-11 (1)	*DEVELOPER SECURITY TESTING AND EVALUATION | CODE ANALYSIS TOOLS*		X			
SA-11 (2)	*DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES*		X			
SA-11 (3)	*DEVELOPER SECURITY TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE*		X			
SA-11 (4)	*DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS*		X			
SA-11 (5)	*DEVELOPER SECURITY TESTING AND EVALUATION | PENETRATION TESTING / ANALYSIS*		X			
SA-11 (6)	*DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS*		X			
SA-11 (7)	*DEVELOPER SECURITY TESTING AND EVALUATION | VERIFY SCOPE OF TESTING / EVALUATION*		X			
SA-12	**Supply Chain Protection**		X			x
SA-12 (1)	*SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS*		X			
SA-12 (2)	*SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS*		X			
SA-12 (3)	*SUPPLY CHAIN PROTECTION | TRUSTED SHIPPING AND WAREHOUSING*	X	Incorporated into SA-12 (1).			
SA-12 (4)	*SUPPLY CHAIN PROTECTION | DIVERSITY OF SUPPLIERS*	X	Incorporated into SA-12 (13).			
SA-12 (5)	*SUPPLY CHAIN PROTECTION | LIMITATION OF HARM*		X			
SA-12 (6)	*SUPPLY CHAIN PROTECTION | MINIMIZING PROCUREMENT TIME*	X	Incorporated into SA-12 (1).			
SA-12 (7)	*SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE*		X			
SA-12 (8)	*SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE*		X			
SA-12 (9)	*SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY*		X			
SA-12 (10)	*SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED*		X			
SA-12 (11)	*SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS*		X			
SA-12 (12)	*SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS*		X			
SA-12 (13)	*SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS*		X			
SA-12 (14)	*SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY*		X			
SA-12 (15)	*SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES*		X			
SA-13	**Trustworthiness**		X			
SA-14	**Criticality Analysis**		X			
SA-14 (1)	*CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING*	X	Incorporated into SA-20.			

Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: / *FLAW REMEDIATION*
Deleted: A
Deleted: *TESTING / RESULTS*
Deleted: A
Deleted: A
Deleted: SA-11 (6) …
Deleted: 7
Deleted: A
Deleted: 8
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: W
Deleted: .
Deleted: W
Deleted: .
Deleted: A
Deleted: W
Deleted: .
Deleted: A
Deleted: A
Deleted: A
Deleted: SA-12 (10) …
Deleted: 11
Deleted: A
Deleted: 12
Deleted: A
Deleted: *SUPPLY CHAIN*
Deleted: 13
Deleted: A
Deleted: 14
Deleted: A
Deleted: A
Deleted: W
Deleted: Incorporated into Appendix E.
Deleted: Critical Information System …
Deleted: A
Deleted: *SUPPLY CHAIN PROTECTION* |
Deleted: W
Deleted: 12

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-15	**Development Process, Standards, and Tools**		X			X
SA-15 (1)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | QUALITY METRICS*		X			
SA-15 (2)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY TRACKING TOOLS*		X			
SA-15 (3)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS*		X			
SA-15 (4)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING / VULNERABILITY ANALYSIS*		X			
SA-15 (5)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION*		X			
SA-15 (6)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT*		X			
SA-15 (7)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS*		X			
SA-15 (8)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT / VULNERABILITY INFORMATION*		X			
SA-15 (9)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | USE OF LIVE DATA*		X			
SA-15 (10)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | INCIDENT RESPONSE PLAN*		X			
SA-15 (11)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ARCHIVE INFORMATION SYSTEM / COMPONENT*		X			
SA-16	**Developer-Provided Training**		X			X
SA-17	**Developer Security Architecture and Design**		X			X
SA-17 (1)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL*		X			
SA-17 (2)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | SECURITY-RELEVANT COMPONENTS*		X			
SA-17 (3)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE*		X			
SA-17 (4)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE*		X			
SA-17 (5)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | CONCEPTUALLY SIMPLE DESIGN*		X			
SA-17 (6)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING*		X			
SA-17 (7)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE*		X			
SA-18	**Tamper Resistance and Detection**		X			
SA-18 (1)	*TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC*		X			
SA-18 (2)	*TAMPER RESISTANCE AND DETECTION | INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES*		X			
SA-19	**Component Authenticity**		X			
SA-19 (1)	*COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*		X			
SA-19 (2)	*COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR*		X			
SA-19 (3)	*COMPONENT AUTHENTICITY | COMPONENT DISPOSAL*		X			
SA-19 (4)	*COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*		X			
SA-20	**Customized Development of Critical Components**		X			
SA-21	**Developer Screening**		X			

Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: Anti-Counterfeit
Deleted: A

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-21 (1)	*DEVELOPER SCREENING | VALIDATION OF SCREENING*		X			

TABLE D-18: SUMMARY — SYSTEM AND COMMUNICATIONS PROTECTION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-1	**System and Communications Protection Policy and Procedures**		x	x	x	x
SC-2	**Application Partitioning**		x		x	x
SC-2 (1)	*APPLICATION PARTITIONING | INTERFACES FOR NON-PRIVILEGED USERS*		x			
SC-3	**Security Function Isolation**		x			x
SC-3 (1)	*SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION*		x			
SC-3 (2)	*SECURITY FUNCTION ISOLATION | ACCESS / FLOW CONTROL FUNCTIONS*		x			
SC-3 (3)	*SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY*		x			
SC-3 (4)	*SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS*		x			
SC-3 (5)	*SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES*		x			
SC-3 (6)	*SECURITY FUNCTION ISOLATION | BOUNDARY PROTECTION MECHANISMS*	x	Incorporated into SC-7 (21).			
SC-3 (7)	*SECURITY FUNCTION ISOLATION | MODULE COHESION*		x			
SC-4	**Information in Shared Resources**				x	x
SC-4 (1)	*INFORMATION IN SHARED RESOURCES | SECURITY LEVELS*	x	Incorporated into SC-4.			
SC-4 (2)	*INFORMATION IN SHARED RESOURCES | PERIODS PROCESSING*					
SC-5	**Denial of Service Protection**			x	x	x
SC-5 (1)	*DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS*					
SC-5 (2)	*DENIAL OF SERVICE PROTECTION | EXCESS CAPACITY / BANDWIDTH / REDUNDANCY*					
SC-5 (3)	*DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING*					
SC-6	**Resource Availability**		x			
SC-7	**Boundary Protection**			x	x	x
SC-7 (1)	*BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS*	x	Incorporated into SC-7.			
SC-7 (2)	*BOUNDARY PROTECTION | PUBLIC ACCESS*	x	Incorporated into SC-7.			
SC-7 (3)	*BOUNDARY PROTECTION | ACCESS POINTS*				x	x
SC-7 (4)	*BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*				x	x
SC-7 (5)	*BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*				x	x
SC-7 (6)	*BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES*	x	Incorporated into SC-7 (18).			
SC-7 (7)	*BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES*				x	x
SC-7 (8)	*BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*					x
SC-7 (9)	*BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC*					
SC-7 (10)	*BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION*					
SC-7 (11)	*BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC*					
SC-7 (12)	*BOUNDARY PROTECTION | HOST-BASED PROTECTION*					
SC-7 (13)	*BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS*					
SC-7 (14)	*BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS*					

Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: W
Deleted: *CLASSIFICATION LEVELS / SECURITY CATEGORIES*
Deleted: A
Deleted: x
Deleted: W
Deleted: x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-7 (15)	*BOUNDARY PROTECTION | ROUTE PRIVILEGED NETWORK ACCESSES*					
SC-7 (16)	*BOUNDARY PROTECTION | PREVENT DISCOVERY OF COMPONENTS / DEVICES*					
SC-7 (17)	*BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS*					
SC-7 (18)	*BOUNDARY PROTECTION | FAIL SECURE*					
SC-7 (19)	*BOUNDARY PROTECTION | BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS*					
SC-7 (20)	*BOUNDARY PROTECTION | DYNAMIC ISOLATION / SEGREGATION*					
SC-7 (21)	*BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS*		X			X
SC-7 (22)	*BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS*		X			
SC-7 (23)	*BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE*					
SC-8	**Transmission Confidentiality and Integrity**				x	x
SC-8 (1)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*				x	x
SC-8 (2)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE / POST TRANSMISSION HANDLING*					
SC-8 (3)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS*					
SC-8 (4)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL / RANDOMIZE COMMUNICATIONS*					
SC-9	**Transmission Confidentiality**	X	Incorporated into SC-8.			
SC-9 (1)	*TRANSMISSION CONFIDENTIALITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*	X	Incorporated into SC-8 (1).			
SC-9 (2)	*TRANSMISSION CONFIDENTIALITY | PRE / POST TRANSMISSION HANDLING*	X	Incorporated into SC-8 (2).			
SC-9 (3)	*TRANSMISSION CONFIDENTIALITY | CRYPTOGRAPHIC OR ALTERNATIVE PROTECTION FOR MESSAGE EXTERNALS*	X	Incorporated into SC-8 (3).			
SC-9 (4)	*TRANSMISSION CONFIDENTIALITY | CONCEAL / RANDOMIZE COMMUNICATIONS*	X	Incorporated into SC-8 (4).			
SC-10	**Network Disconnect**				x	x
SC-11	**Trusted Path**		X			
SC-11 (1)	*TRUSTED PATH | LOGICAL ISOLATION*		X			
SC-12	**Cryptographic Key Establishment and Management**			x	x	x
SC-12 (1)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*					x
SC-12 (2)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS*					
SC-12 (3)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS*					
SC-12 (4)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES*	X	Incorporated into SC-12.			
SC-12 (5)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS*	X	Incorporated into SC-12.			
SC-13	**Cryptographic Protection**			x	x	x
SC-13 (1)	*CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY*	X	Incorporated into SC-13.			
SC-13 (2)	*CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY*	X	Incorporated into SC-13.			
SC-13 (3)	*CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL*	X	Incorporated into SC-13.			

Deleted: *BLOCKING INBOUND / OUTBOUND COMMUNICATIONS TRAFFIC*

Deleted: *INTEGRITY PRIOR TO*

Deleted: x

Deleted: x

Deleted: *PRIOR TO*

Deleted: A

Deleted: W

Deleted: W

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
	ACCESS APPROVALS					
SC-13 (4)	*CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES*	X	Incorporated into SC-13.			
SC-14	**Public Access Protections**	X	Capability provided by AC-3, SI-3, SI-4, SI-5, SI-7, SI-9, SI-10.			
SC-15	**Collaborative Computing Devices**			x	x	x
SC-15 (1)	*COLLABORATIVE COMPUTING DEVICES | PHYSICAL DISCONNECT*					
SC-15 (2)	*COLLABORATIVE COMPUTING DEVICES | BLOCKING INBOUND / OUTBOUND COMMUNICATIONS TRAFFIC*	X	Incorporated into SC-7.			
SC-15 (3)	*COLLABORATIVE COMPUTING DEVICES | DISABLING / REMOVAL IN SECURE WORK AREAS*					
SC-15 (4)	*COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS*					
SC-16	**Transmission of Security Attributes**					
SC-16 (1)	*TRANSMISSION OF SECURITY ATTRIBUTES | INTEGRITY VALIDATION*					
SC-17	**Public Key Infrastructure Certificates**				x	x
SC-18	**Mobile Code**				x	x
SC-18 (1)	*MOBILE CODE | IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS*					
SC-18 (2)	*MOBILE CODE | ACQUISITION / DEVELOPMENT / USE*					
SC-18 (3)	*MOBILE CODE | PREVENT DOWNLOADING / EXECUTION*					
SC-18 (4)	*MOBILE CODE | PREVENT AUTOMATIC EXECUTION*					
SC-18 (5)	*MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS*					
SC-19	**Voice Over Internet Protocol**				x	x
SC-20	**Secure Name /Address Resolution Service (Authoritative Source)**			x	x	x
SC-20 (1)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES*	X	Incorporated into SC-20.			
SC-20 (2)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN / INTEGRITY*					
SC-21	**Secure Name /Address Resolution Service (Recursive or Caching Resolver)**			x	x	x
SC-21 (1)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | DATA ORIGIN / INTEGRITY*	X	Incorporated into SC-21.			
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**			x	x	x
SC-23	**Session Authenticity**				x	x
SC-23 (1)	*SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT*					
SC-23 (2)	*SESSION AUTHENTICITY | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS*					
SC-23 (3)	*SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*					
SC-23 (4)	*SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*	X	Incorporated into SC-23 (3).			
SC-23 (5)	*SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES*					
SC-24	**Fail in Known State**		X			x
SC-25	**Thin Nodes**					
SC-26	**Honeypots**					
SC-26 (1)	*HONEYPOTS | DETECTION OF MALICIOUS CODE*	X	Incorporated into SC-35.			

Deleted: x

Deleted: W

Deleted: *IN*

Deleted: W

Deleted: W

Deleted: A

Deleted: W

Deleted: 36

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-27	**Platform-Independent Applications**					
SC-28	**Protection of Information at Rest**				x	x
SC-28 (1)	*PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION*					
SC-28 (2)	*PROTECTION OF INFORMATION AT REST | OFF-LINE STORAGE*					
SC-29	**Heterogeneity**					
SC-29 (1)	*HETEROGENEITY | VIRTUALIZATION TECHNIQUES*					
SC-30	**Concealment and Misdirection**					
SC-30 (1)	*CONCEALMENT AND MISDIRECTION | VIRTUALIZATION TECHNIQUES*	x	Incorporated into SC-29 (1).			
SC-30 (2)	*CONCEALMENT AND MISDIRECTION | RANDOMNESS*					
SC-30 (3)	*CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING / STORAGE LOCATIONS*					
SC-30 (4)	*CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION*					
SC-30 (5)	*CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS*					
SC-31	**Covert Channel Analysis**					
SC-31 (1)	*COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY*					
SC-31 (2)	*COVERT CHANNEL ANALYSIS | MAXIMUM BANDWIDTH*					
SC-31 (3)	*COVERT CHANNEL ANALYSIS | MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS*					
SC-32	**Information System Partitioning**					
SC-33	**Transmission Preparation Integrity**	x	Incorporated into SC-8.			
SC-34	**Non-Modifiable Executable Programs**					
SC-34 (1)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE*					
SC-34 (2)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION / READ-ONLY MEDIA*					
SC-34 (3)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION*					
SC-35	**Honeyclients**					
SC-36	**Distributed Processing and Storage**					
SC-36 (1)	*DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES*					
SC-37	**Out-of-Band Channels**					
SC-37 (1)	*OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION*					
SC-38	**Operations Security**					
SC-39	**Process Isolation**			x	x	x
SC-39 (1)	*PROCESS ISOLATION | HARDWARE SEPARATION*					
SC-39 (2)	*PROCESS ISOLATION | THREAD ISOLATION*					
SC-40	**Wireless Link Protection**					
SC-40 (1)	*WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE*					
SC-40 (2)	*WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL*					
SC-40 (3)	*WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION*					
SC-40 (4)	*WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION*					
SC-41	**Port and I/O Device Access**					
SC-42	**Sensor Data**					
SC-42 (1)	*SENSOR DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES*					
SC-42 (2)	*SENSOR DATA | AUTHORIZED USE*					

Deleted: Operating System
Deleted: A
Deleted: A
Deleted: A
Deleted: W
Deleted: .
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: TESTING OF DEVELOPER-IDENTIFIED
Deleted: W
Deleted: Incorporated into SC-31.
Deleted: A
Deleted: A
Deleted: A
Deleted: x
Deleted: x
Deleted: W
Deleted: A
Deleted: A
Deleted: A
Deleted: 35
Moved up [19]: Technical Surveillance ...
Deleted: 36
Deleted: 37
Deleted: A
Deleted: SC-37 (1) ...
Deleted: 37 (2
Deleted: A
Deleted: SC-38 ...
Deleted: 39
Deleted: A
Deleted: 39
Deleted: A
Deleted: 40
Deleted: A
Deleted: 41
Deleted: A
Deleted: 41
Deleted: A
Deleted: 42
Deleted: 42
Deleted: 42
Deleted: 42
Deleted: 42

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-43	Usage Restrictions					
SC-44	Detonation Chambers					

TABLE D-19: SUMMARY — SYSTEM AND INFORMATION INTEGRITY CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SI-1	**System and Information Integrity Policy and Procedures**		x	x	x	x
SI-2	**Flaw Remediation**			x	x	x
SI-2 (1)	*FLAW REMEDIATION | CENTRAL MANAGEMENT*					x
SI-2 (2)	*FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS*				x	x
SI-2 (3)	*FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS*					
SI-2 (4)	*FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS*	x	Incorporated into SI-2.			
SI-2 (5)	*FLAW REMEDIATION | AUTOMATIC SOFTWARE / FIRMWARE UPDATES*					
SI-2 (6)	*FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE*					
SI-3	**Malicious Code Protection**			x	x	x
SI-3 (1)	*MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT*				x	x
SI-3 (2)	*MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES*				x	x
SI-3 (3)	*MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS*	x	Incorporated into AC-6 (10).			
SI-3 (4)	*MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED USERS*					
SI-3 (5)	*MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES*	x	Incorporated into MP-7.			
SI-3 (6)	*MALICIOUS CODE PROTECTION | TESTING / VERIFICATION*					
SI-3 (7)	*MALICIOUS CODE PROTECTION | NON SIGNATURE-BASED DETECTION*					
SI-3 (8)	*MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS*					
SI-3 (9)	*MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS*					
SI-3 (10)	*MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS*					
SI-4	**Information System Monitoring**		x	x	x	x
SI-4 (1)	*INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM*		x			
SI-4 (2)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*		x		x	x
SI-4 (3)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOL INTEGRATION*		x			
SI-4 (4)	*INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*		x		x	x
SI-4 (5)	*INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*		x		x	x
SI-4 (6)	*INFORMATION SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS*	x	Incorporated into AC-6 (10).			
SI-4 (7)	*INFORMATION SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS*		x			
SI-4 (8)	*INFORMATION SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION*	x	Incorporated into SI-4.			
SI-4 (9)	*INFORMATION SYSTEM MONITORING | TESTING OF MONITORING TOOLS*		x			
SI-4 (10)	*INFORMATION SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS*		x			
SI-4 (11)	*INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES*		x			
SI-4 (12)	*INFORMATION SYSTEM MONITORING | AUTOMATED ALERTS*		x			
SI-4 (13)	*INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS*		x			
SI-4 (14)	*INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION*		x			

Deleted: A
Deleted: AND AUTOMATIC SOFTWARE / FIRMWARE UPDATES
Deleted: W
Deleted: x
Deleted: REMOVABLE MEDIA
Deleted: W
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: NEAR REAL-TIME
Deleted: A
Deleted: x
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SI-4 (15)	*INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS*		X			
SI-4 (16)	*INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION*		X			
SI-4 (17)	*INFORMATION SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS*		X			
SI-4 (18)	*INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / COVERT EXFILTRATION*		X			
SI-4 (19)	*INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK*		X			
SI-4 (20)	*INFORMATION SYSTEM MONITORING | PRIVILEGED USER*		X			
SI-4 (21)	*INFORMATION SYSTEM MONITORING | PROBATIONARY PERIODS*		X			
SI-4 (22)	*INFORMATION SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES*		X			
SI-4 (23)	*INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES*		X			
SI-4 (24)	*INFORMATION SYSTEM MONITORING | INDICATORS OF COMPROMISE*		X			
SI-5	**Security Alerts, Advisories, and Directives**		X	X	X	X
SI-5 (1)	*SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES*		X			X
SI-6	**Security Function Verification**		X			X
SI-6 (1)	*SECURITY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS*	X	Incorporated into SI-6.			
SI-6 (2)	*SECURITY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING*					
SI-6 (3)	*SECURITY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS*					
SI-7	**Software, Firmware, and Information Integrity**		X		X	X
SI-7 (1)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*		X		X	X
SI-7 (2)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS*		X			X
SI-7 (3)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY-MANAGED INTEGRITY TOOLS*		X			
SI-7 (4)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER-EVIDENT PACKAGING*	X	Incorporated into SA-12.			
SI-7 (5)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS*		X			X
SI-7 (6)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION*		X			
SI-7 (7)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*		X		X	X
SI-7 (8)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS*		X			
SI-7 (9)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS*		X			
SI-7 (10)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE*		X			
SI-7 (11)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES*		X			
SI-7 (12)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION*		X			

Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: A
Deleted: W
Deleted: A
Deleted: A
Deleted: SCANS
Deleted: A
Deleted: A
Deleted: W
Deleted: A
Deleted: A
Deleted: SI-7 (7)
Deleted: 8
Deleted: A
Deleted: 9
Deleted: A
Deleted: 10
Deleted: A
Deleted: 11
Deleted: A
Deleted: 12
Deleted: A
Deleted: 13
Deleted: A

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SI-7 (13)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS*		X			
SI-7 (14)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*		X			X
SI-7 (15)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION*		X			
SI-7 (16)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*		X			
SI-8	**Spam Protection**				X	X
SI-8 (1)	*SPAM PROTECTION | CENTRAL MANAGEMENT OF PROTECTION MECHANISMS*				X	X
SI-8 (2)	*SPAM PROTECTION | AUTOMATIC UPDATES*				X	X
SI-8 (3)	*SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY*					
SI-9	**Information Input Restrictions**	X	Incorporated into AC-2, AC-3, AC-5, AC-6.			
SI-10	**Information Input Validation**		X		X	X
SI-10 (1)	*INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY*		X			
SI-10 (2)	*INFORMATION INPUT VALIDATION | REVIEW / RESOLUTION OF ERRORS*		X			
SI-10 (3)	*INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR*		X			
SI-10 (4)	*INFORMATION INPUT VALIDATION | REVIEW / TIMING INTERACTIONS*		X			
SI-10 (5)	*INFORMATION INPUT VALIDATION | REVIEW / RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS*		X			
SI-11	**Error Handling**				X	X
SI-12	**Information Handling and Retention**			X	X	X
SI-13	**Predictable Failure Prevention**		X			
SI-13 (1)	*PREDICTABLE FAILURE PREVENTION | TRANSFERRING COMPONENT RESPONSIBILITIES*		X			
SI-13 (2)	*PREDICTABLE FAILURE PREVENTION | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*	X	Incorporated into SI-7 (16).			
SI-13 (3)	*PREDICTABLE FAILURE PREVENTION | MANUAL TRANSFER BETWEEN COMPONENTS*		X			
SI-13 (4)	*PREDICTABLE FAILURE PREVENTION | STANDBY COMPONENT INSTALLATION / NOTIFICATION*		X			
SI-13 (5)	*PREDICTABLE FAILURE PREVENTION | FAILOVER CAPABILITY*		X			
SI-14	**Non-Persistence**		X			
SI-14 (1)	*NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES*		X			
SI-15	**Information Output Filtering**		X			
SI-16	**Memory Protection**		X		X	X

Deleted: 14
Deleted: A
Deleted: 15
Deleted: A
Deleted: x
Deleted: SI-9 (1)
Deleted: A
Deleted: Output
Deleted: W
Deleted: Incorporated into CP-11.
Moved (insertion) [20]
Moved (insertion) [21]
Moved (insertion) [22]
Moved (insertion) [23]
Deleted: A

ADJUSTMENTS TO SECURITY CONTROL BASELINES

ALLOCATION OF SECURITY CONTROLS AND ASSIGNMENT OF PRIORITY SEQUENCING CODES

With each revision to SP 800-53, minor adjustments may occur with the security control baselines including, for example, allocating additional controls and/or control enhancements, eliminating selected controls/enhancements, and changing sequencing priority codes (P-codes). These changes reflect: (i) the ongoing receipt and analysis of threat information; (ii) the periodic reexamination of the initial assumptions that generated the security control baselines; (iii) the desire for common security control baseline starting points for national security and non national security systems to achieve community-wide convergence (relying subsequently on specific overlays to describe any adjustments from the common starting points); and (iv) the periodic reassessment of priority codes to appropriately balance the workload of security control implementation. Over time, as the security control catalog expands to address the continuing challenges from a dynamic and growing threat space that is increasingly sophisticated, organizations will come to rely to a much greater degree on overlays to provide the needed specialization for their security plans.