

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.⁹⁰ The three security control baselines are hierarchical in nature with regard to the security controls employed in those baselines.⁹¹ 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, the IR-2 (1) (2) entry in the high baseline for IR-2 indicates that the second control from the Incident Response family has been selected along with control enhancements (1) and (2). Some security controls and enhancements 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.

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

⁹⁰ 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>.

⁹¹ 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).

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 BASELINES⁹²

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) (11) (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	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	Withdrawn	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	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	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	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
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

⁹² 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.

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
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	P2	Not Selected	Not Selected	AU-10
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	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P2	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 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
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	P2	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) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
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	P2	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
IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1) (2)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
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	P2	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 Analysis Team	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	P3	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	P2	MA-4	MA-4 (2)	MA-4 (2) (3)
MA-5	Maintenance Personnel	P2	MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance	P2	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	P2	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	P2	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	P2	PE-16	PE-16	PE-16

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
PE-17	Alternate Work Site	P2	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P3	Not Selected	Not Selected	PE-18
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
PE-20	Asset Monitoring and Tracking	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	P2	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	P1	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	P1	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) (9) (10)	SA-4 (1) (2) (9) (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)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P0	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
SA-22	Unsupported System Components	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) (18) (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	P2	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

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
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	P0	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 Capability and 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	P2	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
SI-17	Fail-Safe Procedures	P0	Not Selected	Not Selected	Not Selected

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 that have been selected for the security control baselines as indicated by an “x” in the column for the selected baseline;⁹³ (ii) the security controls and control enhancements that have not been selected for any security control baseline (i.e., the controls and control enhancements available for selection to achieve greater protection) as indicated by blank cells in the baseline columns; (iii) the security controls and control enhancements that have been withdrawn from Appendix F as indicated by an “x” in the respective withdrawn column; and (iv) the security controls and control enhancements that have assurance-related characteristics or properties (i.e., assurance-related controls) as indicated by an “x” in the respective assurance column. 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).

⁹³ 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.

TABLE D-3: SUMMARY — ACCESS CONTROLS

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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 / GROUP 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					X
AC-2(13)	ACCOUNT MANAGEMENT DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS					X
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.			
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					

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
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 APPROVED SOLUTIONS					
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					
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	X

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-12(1)	SESSION TERMINATION USER-INITIATED LOGOUTS / MESSAGE DISPLAYS					
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 SI-4.			
AC-17(6)	REMOTE ACCESS PROTECTION OF INFORMATION					
AC-17(7)	REMOTE ACCESS ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS	X	Incorporated into AC-3(10).			
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.			

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
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			

TABLE D-4: SUMMARY — AWARENESS AND TRAINING CONTROLS

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

TABLE D-5: SUMMARY — AUDIT AND ACCOUNTABILITY CONTROLS

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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(9).			
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					

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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			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-11(1)	AUDIT RECORD RETENTION LONG-TERM RETRIEVAL CAPABILITY		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 CAPTURE/RECORD AND LOG CONTENT		X			
AU-14(3)	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					

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

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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)	<i>SECURITY ASSESSMENTS INDEPENDENT ASSESSORS</i>		X		X	X
CA-2(2)	<i>SECURITY ASSESSMENTS SPECIALIZED ASSESSMENTS</i>		X			X
CA-2(3)	<i>SECURITY ASSESSMENTS EXTERNAL ORGANIZATIONS</i>		X			
CA-3	System Interconnections		X	X	X	X
CA-3(1)	<i>SYSTEM INTERCONNECTIONS UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS</i>					
CA-3(2)	<i>SYSTEM INTERCONNECTIONS CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS</i>					
CA-3(3)	<i>SYSTEM INTERCONNECTIONS UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS</i>					
CA-3(4)	<i>SYSTEM INTERCONNECTIONS CONNECTIONS TO PUBLIC NETWORKS</i>					
CA-3(5)	<i>SYSTEM INTERCONNECTIONS RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS</i>				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)	<i>PLAN OF ACTION AND MILESTONES AUTOMATION SUPPORT FOR ACCURACY / CURRENCY</i>		X			
CA-6	Security Authorization		X	X	X	X
CA-7	Continuous Monitoring		X	X	X	X
CA-7(1)	<i>CONTINUOUS MONITORING INDEPENDENT ASSESSMENT</i>		X		X	X
CA-7(2)	<i>CONTINUOUS MONITORING TYPES OF ASSESSMENTS</i>	X	Incorporated into CA-2.			
CA-7(3)	<i>CONTINUOUS MONITORING TREND ANALYSES</i>		X			
CA-8	Penetration Testing		X			X
CA-8(1)	<i>PENETRATION TESTING INDEPENDENT PENETRATION AGENT OR TEAM</i>		X			
CA-8(2)	<i>PENETRATION TESTING RED TEAM EXERCISES</i>		X			
CA-9	Internal System Connections		X	X	X	X
CA-9(1)	<i>INTERNAL SYSTEM CONNECTIONS SECURITY COMPLIANCE CHECKS</i>		X			

TABLE D-7: SUMMARY — CONFIGURATION MANAGEMENT CONTROLS

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

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
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 NO DUPLICATE ACCOUNTING OF COMPONENTS		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					

TABLE D-8: SUMMARY — CONTINGENCY PLANNING CONTROLS

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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

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

TABLE D-9: SUMMARY — IDENTIFICATION AND AUTHENTICATION CONTROLS

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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 - SEPARATE DEVICE				X	X
IA-2(12)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) ACCEPTANCE OF PIV CREDENTIALS			X	X	X
IA-2(13)	IDENTIFICATION AND AUTHENTICATION OUT-OF-BAND AUTHENTICATION					
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

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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-BASED 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					

TABLE D-10: SUMMARY — INCIDENT RESPONSE CONTROLS

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

TABLE D-11: SUMMARY — MAINTENANCE CONTROLS

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

TABLE D-12: SUMMARY — MEDIA PROTECTION CONTROLS

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

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

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

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PE-12	Emergency Lighting			X	X	X
PE-12(1)	<i>EMERGENCY LIGHTING ESSENTIAL MISSIONS / BUSINESS FUNCTIONS</i>					
PE-13	Fire Protection			X	X	X
PE-13(1)	<i>FIRE PROTECTION DETECTION DEVICES / SYSTEMS</i>					X
PE-13(2)	<i>FIRE PROTECTION SUPPRESSION DEVICES / SYSTEMS</i>					X
PE-13(3)	<i>FIRE PROTECTION AUTOMATIC FIRE SUPPRESSION</i>				X	X
PE-13(4)	<i>FIRE PROTECTION INSPECTIONS</i>					
PE-14	Temperature and Humidity Controls			X	X	X
PE-14(1)	<i>TEMPERATURE AND HUMIDITY CONTROLS AUTOMATIC CONTROLS</i>					
PE-14(2)	<i>TEMPERATURE AND HUMIDITY CONTROLS MONITORING WITH ALARMS / NOTIFICATIONS</i>					
PE-15	Water Damage Protection			X	X	X
PE-15(1)	<i>WATER DAMAGE PROTECTION AUTOMATION SUPPORT</i>					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)	<i>LOCATION OF INFORMATION SYSTEM COMPONENTS FACILITY SITE</i>					
PE-19	Information Leakage					
PE-19(1)	<i>INFORMATION LEAKAGE NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES</i>					
PE-20	Asset Monitoring and Tracking					

TABLE D-14: SUMMARY — PLANNING CONTROLS

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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)	<i>SYSTEM SECURITY PLAN CONCEPT OF OPERATIONS</i>	X	Incorporated into PL-7.			
PL-2(2)	<i>SYSTEM SECURITY PLAN FUNCTIONAL ARCHITECTURE</i>	X	Incorporated into PL-8.			
PL-2(3)	<i>SYSTEM SECURITY PLAN PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES</i>		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)	<i>RULES OF BEHAVIOR SOCIAL MEDIA AND NETWORKING RESTRICTIONS</i>		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)	<i>INFORMATION SECURITY ARCHITECTURE DEFENSE-IN-DEPTH</i>		X			
PL-8(2)	<i>INFORMATION SECURITY ARCHITECTURE SUPPLIER DIVERSITY</i>		X			
PL-9	Central Management		X			

TABLE D-15: SUMMARY — PERSONNEL SECURITY CONTROLS

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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)	<i>PERSONNEL SCREENING CLASSIFIED INFORMATION</i>					
PS-3(2)	<i>PERSONNEL SCREENING FORMAL INDOCTRINATION</i>					
PS-3(3)	<i>PERSONNEL SCREENING INFORMATION WITH SPECIAL PROTECTION MEASURES</i>					
PS-4	Personnel Termination			X	X	X
PS-4(1)	<i>PERSONNEL TERMINATION POST-EMPLOYMENT REQUIREMENTS</i>					
PS-4(2)	<i>PERSONNEL TERMINATION AUTOMATED NOTIFICATION</i>					X
PS-5	Personnel Transfer			X	X	X
PS-6	Access Agreements		X	X	X	X
PS-6(1)	<i>ACCESS AGREEMENTS INFORMATION REQUIRING SPECIAL PROTECTION</i>	X	Incorporated into PS-3.			
PS-6(2)	<i>ACCESS AGREEMENTS CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION</i>		X			
PS-6(3)	<i>ACCESS AGREEMENTS POST-EMPLOYMENT REQUIREMENTS</i>		X			
PS-7	Third-Party Personnel Security		X	X	X	X
PS-8	Personnel Sanctions			X	X	X

TABLE D-16: SUMMARY — RISK ASSESSMENT CONTROLS

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

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

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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-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			
SA-10(2)	DEVELOPER CONFIGURATION MANAGEMENT ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES		X			

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
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 STATIC CODE ANALYSIS		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		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-11(8)	DEVELOPER SECURITY TESTING AND EVALUATION DYNAMIC CODE ANALYSIS		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.			

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

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-21(1)	<i>DEVELOPER SCREENING VALIDATION OF SCREENING</i>		X			
SA-22	Unsupported System Components		X			
SA-22(1)	<i>UNSUPPORTED SYSTEM COMPONENTS ALTERNATIVE SOURCES FOR CONTINUED SUPPORT</i>		X			

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

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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)	<i>APPLICATION PARTITIONING INTERFACES FOR NON-PRIVILEGED USERS</i>		X			
SC-3	Security Function Isolation		X			X
SC-3(1)	<i>SECURITY FUNCTION ISOLATION HARDWARE SEPARATION</i>		X			
SC-3(2)	<i>SECURITY FUNCTION ISOLATION ACCESS / FLOW CONTROL FUNCTIONS</i>		X			
SC-3(3)	<i>SECURITY FUNCTION ISOLATION MINIMIZE NONSECURITY FUNCTIONALITY</i>		X			
SC-3(4)	<i>SECURITY FUNCTION ISOLATION MODULE COUPLING AND COHESIVENESS</i>		X			
SC-3(5)	<i>SECURITY FUNCTION ISOLATION LAYERED STRUCTURES</i>		X			
SC-4	Information in Shared Resources				X	X
SC-4(1)	<i>INFORMATION IN SHARED RESOURCES SECURITY LEVELS</i>	X	Incorporated into SC-4.			
SC-4(2)	<i>INFORMATION IN SHARED RESOURCES PERIODS PROCESSING</i>					
SC-5	Denial of Service Protection			X	X	X
SC-5(1)	<i>DENIAL OF SERVICE PROTECTION RESTRICT INTERNAL USERS</i>					
SC-5(2)	<i>DENIAL OF SERVICE PROTECTION EXCESS CAPACITY / BANDWIDTH / REDUNDANCY</i>					
SC-5(3)	<i>DENIAL OF SERVICE PROTECTION DETECTION / MONITORING</i>					
SC-6	Resource Availability		X			
SC-7	Boundary Protection			X	X	X
SC-7(1)	<i>BOUNDARY PROTECTION PHYSICALLY SEPARATED SUBNETWORKS</i>	X	Incorporated into SC-7.			
SC-7(2)	<i>BOUNDARY PROTECTION PUBLIC ACCESS</i>	X	Incorporated into SC-7.			
SC-7(3)	<i>BOUNDARY PROTECTION ACCESS POINTS</i>				X	X
SC-7(4)	<i>BOUNDARY PROTECTION EXTERNAL TELECOMMUNICATIONS SERVICES</i>				X	X
SC-7(5)	<i>BOUNDARY PROTECTION DENY BY DEFAULT / ALLOW BY EXCEPTION</i>				X	X
SC-7(6)	<i>BOUNDARY PROTECTION RESPONSE TO RECOGNIZED FAILURES</i>	X	Incorporated into SC-7(18).			
SC-7(7)	<i>BOUNDARY PROTECTION PREVENT SPLIT TUNNELING FOR REMOTE DEVICES</i>				X	X
SC-7(8)	<i>BOUNDARY PROTECTION ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS</i>					X
SC-7(9)	<i>BOUNDARY PROTECTION RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC</i>					
SC-7(10)	<i>BOUNDARY PROTECTION PREVENT UNAUTHORIZED EXFILTRATION</i>					
SC-7(11)	<i>BOUNDARY PROTECTION RESTRICT INCOMING COMMUNICATIONS TRAFFIC</i>					
SC-7(12)	<i>BOUNDARY PROTECTION HOST-BASED PROTECTION</i>					
SC-7(13)	<i>BOUNDARY PROTECTION ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS</i>					
SC-7(14)	<i>BOUNDARY PROTECTION PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS</i>					
SC-7(15)	<i>BOUNDARY PROTECTION ROUTE PRIVILEGED NETWORK ACCESSES</i>					
SC-7(16)	<i>BOUNDARY PROTECTION PREVENT DISCOVERY OF COMPONENTS / DEVICES</i>					

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-7(17)	BOUNDARY PROTECTION AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS					
SC-7(18)	BOUNDARY PROTECTION FAIL SECURE		X			X
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-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 ACCESS APPROVALS	X	Incorporated into SC-13.			
SC-13(4)	CRYPTOGRAPHIC PROTECTION DIGITAL SIGNATURES	X	Incorporated into SC-13.			
SC-14	Public Access Protections	X	Capability provided by AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7, 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					

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
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	X	Incorporated into AC-12(1).			
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.			
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		X			
SC-29(1)	HETEROGENEITY VIRTUALIZATION TECHNIQUES		X			
SC-30	Concealment and Misdirection		X			
SC-30(1)	CONCEALMENT AND MISDIRECTION VIRTUALIZATION TECHNIQUES	X	Incorporated into SC-29(1).			

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-30(2)	CONCEALMENT AND MISDIRECTION RANDOMNESS		X			
SC-30(3)	CONCEALMENT AND MISDIRECTION CHANGE PROCESSING / STORAGE LOCATIONS		X			
SC-30(4)	CONCEALMENT AND MISDIRECTION MISLEADING INFORMATION		X			
SC-30(5)	CONCEALMENT AND MISDIRECTION CONCEALMENT OF SYSTEM COMPONENTS		X			
SC-31	Covert Channel Analysis		X			
SC-31(1)	COVERT CHANNEL ANALYSIS TEST COVERT CHANNELS FOR EXPLOITABILITY		X			
SC-31(2)	COVERT CHANNEL ANALYSIS MAXIMUM BANDWIDTH		X			
SC-31(3)	COVERT CHANNEL ANALYSIS MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS		X			
SC-32	Information System Partitioning		X			
SC-33	Transmission Preparation Integrity	X	Incorporated into SC-8.			
SC-34	Non-Modifiable Executable Programs		X			
SC-34(1)	NON-MODIFIABLE EXECUTABLE PROGRAMS NO WRITABLE STORAGE		X			
SC-34(2)	NON-MODIFIABLE EXECUTABLE PROGRAMS INTEGRITY PROTECTION / READ-ONLY MEDIA		X			
SC-34(3)	NON-MODIFIABLE EXECUTABLE PROGRAMS HARDWARE-BASED PROTECTION		X			
SC-35	Honeyclients					
SC-36	Distributed Processing and Storage		X			
SC-36(1)	DISTRIBUTED PROCESSING AND STORAGE POLLING TECHNIQUES		X			
SC-37	Out-of-Band Channels		X			
SC-37(1)	OUT-OF-BAND CHANNELS ENSURE DELIVERY / TRANSMISSION		X			
SC-38	Operations Security		X			
SC-39	Process Isolation		X	X	X	X
SC-39(1)	PROCESS ISOLATION HARDWARE SEPARATION		X			
SC-39(2)	PROCESS ISOLATION THREAD ISOLATION		X			
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 Capability and Data					
SC-42(1)	SENSOR CAPABILITY AND DATA REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES					
SC-42(2)	SENSOR CAPABILITY AND DATA AUTHORIZED USE					
SC-42(3)	SENSOR CAPABILITY AND DATA PROHIBIT USE OF DEVICES					
SC-43	Usage Restrictions					
SC-44	Detonation Chambers					

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

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

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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			

CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	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				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
SI-17	Fail-Safe Procedures		X			

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.