HANDOUT 4

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).

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
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
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

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.

CNTL NO.	CONTROL NAME *Control Enhancement Name*	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 *Control Enhancement Name*	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-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(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*					

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 SYSTEM 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			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	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*					

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**					

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-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-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	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*					

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*					

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			

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	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)	*VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*		x		x	x
RA-5(2)	*VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*		x		x	x
RA-5(3)*	*VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE*		x			
RA-5(4)	*VULNERABILITY SCANNING | DISCOVERABLE INFORMATION*		x			x
RA-5(5)	*VULNERABILITY SCANNING | PRIVILEGED ACCESS*		x		x	x
RA-5(6)	*VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES*		x			
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*		x			
RA-5(9)	*VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES*	x	Incorporated into CA-8.			
RA-5(10)	*VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION*		x			
RA-6	**Technical Surveillance Countermeasures Survey**		x			

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 *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	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 *Control Enhancement Name*	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**					

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			

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.