

APPENDIX D

SECURITY CONTROL TABLES

D.1 NSS SECURITY CONTROL BASELINES

Table D-1 uses a 3-by-3 matrix to identify applicability of security controls in the NIST SP 800-53, Revision 4 baselines for NSS. The matrix also identifies the additional security controls needed to protect NSS. This table represents the security controls applicable to NSS based on impact values.

The 3-by-3 matrix has nine columns showing three possible impact values (low, moderate, or high) for each of the three security objectives (confidentiality, integrity, or availability). The "X"s in the table reflect the NIST specifications by impact value (i.e., low, moderate, and high). The "+"s in the table reflect the additional CNSS specifications by impact value for all NSS. The association of security controls to security objectives is detailed in table D-2. A blank space in the table signifies the control was either not selected or not allocated to a particular security objective for the purposes of this Instruction. Controls that are designated as "withdrawn" indicate that they are no longer in the NIST SP 800-53 security control catalog¹⁰.

Table D-1: NSS Security Control Baselines

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management Removal of Temporary / Emergency Accounts		X	X		X	X			
AC-2(3)	Account Management Disable Inactive Accounts		X	X		X	X			
AC-2(4)	Account Management Automated Audit Actions	+	X	X	+	X	X			
AC-2(5)	Account Management Inactivity Logout	+	+	X	+	+	X	+	+	X
AC-2(6)	Account Management Dynamic Privilege Management									
AC-2(7)	Account Management Role-Based Schemes	+	+	+	+	+	+			
AC-2(8)	Account Management Dynamic Account Creation									
AC-2(9)	Account Management Restrictions on Use of Shared Groups / Accounts	+	+	+	+	+	+			
AC-2(10)	Account Management Shared / Group Account Credential Termination	+	+	+	+	+	+			
AC-2(11)	Account Management Usage Conditions			X			X			
AC-2(12)	Account Management Account Monitoring /	+	+	X	+	+	X			

¹⁰ Changes to the security control catalog are under the authority of NIST.

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
	Atypical Usage									
AC-2(13)	Account Management Disable Accounts For High-Risk Individuals	+	+	X	+	+	X			
AC-3	Access Enforcement	X	X	X	X	X	X			
AC-3(1)	Access Enforcement Restricted Access to Privileged Functions	Withdrawn								
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	Withdrawn								
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		X	X			
AC-4(1)	Information Flow Enforcement Object Security Attributes									
AC-4(2)	Information Flow Enforcement Processing Domains									
AC-4(3)	Information Flow Enforcement Dynamic Information Flow Control									
AC-4(4)	Information Flow Enforcement Content Check Encrypted Information									
AC-4(5)	Information Flow Enforcement Embedded Data Types									
AC-4(6)	Information Flow Enforcement Metadata									
AC-4(7)	Information Flow Enforcement One-Way Flow Mechanisms									
AC-4(8)	Information Flow Enforcement Security Policy Filters									
AC-4(9)	Information Flow Enforcement Human Reviews									
AC-4(10)	Information Flow Enforcement Enable / Disable Security Policy Filters									
AC-4(11)	Information Flow Enforcement Configuration of Security Policy Filters									
AC-4(12)	Information Flow Enforcement Data Type Identifiers									
AC-4(13)	Information Flow Enforcement Decomposition Into Policy-Relevant									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
	Subcomponents									
AC-4(14)	Information Flow Enforcement Security Policy Filter Constraints									
AC-4(15)	Information Flow Enforcement Detection of Unsanctioned Information									
AC-4(16)	<i>Information Flow Enforcement Information Transfers on Interconnected Systems</i>	<i>Withdrawn</i>								
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	+	X	X			
AC-6	Least Privilege	+	X	X	+	X	X			
AC-6(1)	Least Privilege Authorize Access to Security Functions	+	X	X	+	X	X			
AC-6(2)	Least Privilege Non-Privileged Access For Nonsecurity Functions	+	X	X	+	X	X			
AC-6(3)	Least Privilege Network Access to Privileged Commands			X			X			
AC-6(4)	Least Privilege Separate Processing Domains									
AC-6(5)	Least Privilege Privileged Accounts	+	X	X	+	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	+	X	X			
AC-6(10)	Least Privilege Prohibit Nonprivileged Users from Executing Privileged Functions	+	X	X	+	X	X			
AC-7	Unsuccessful Logon Attempts	X	X	X	X	X	X	X	X	X
AC-7(1)	<i>Unsuccessful Logon Attempts Automatic Account Lock</i>	<i>Withdrawn</i>								
AC-7(2)	Unsuccessful Logon Attempts Purge/Wipe Mobile Device									
AC-8	System Use Notification	X	X	X	X	X	X			
AC-9	Previous Logon (Access) Notification									
AC-9(1)	Previous Logon Notification Unsuccessful									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
	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		+	X		+	X
AC-11	Session Lock	+	X	X	+	X	X			
AC-11(1)	Session Lock Pattern-Hiding Displays	+	X	X						
AC-12	Session Termination		X	X		X	X			
AC-12(1)	Session Termination User-initiated Logouts / Message Displays		+	+		+	+			
AC-13	<i>Supervision and Review — Access Control</i>	Withdrawn								
AC-14	Permitted Actions Without Identification or Authentication	X	X	X	X	X	X			
AC-14(1)	<i>Permitted Actions Without Identification or Authentication / Necessary Uses</i>	Withdrawn								
AC-15	<i>Automated Marking</i>	Withdrawn								
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	X	X	X			
AC-17(1)	Remote Access Automated Monitoring / Control	+	X	X	+	X	X			
AC-17(2)	Remote Access Protection of Confidentiality / Integrity Using Encryption	+	X	X	+	X	X			
AC-17(3)	Remote Access Managed Access Control Points	+	X	X	+	X	X			

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-17(4)	Remote Access Privileged Commands / Access	+	X	X	+	X	X			
AC-17(5)	<i>Remote Access Monitoring For Unauthorized Connections</i>	Withdrawn								
AC-17(6)	Remote Access Protection of Information	+	+	+						
AC-17(7)	<i>Remote Access Additional Protection For Security Function Access</i>	Withdrawn								
AC-17(8)	<i>Remote Access Disable Nonsecure Network Protocols</i>	Withdrawn								
AC-17(9)	Remote Access Disconnect / Disable Access	+	+	+	+	+	+			
AC-18	Wireless Access	X	X	X	X	X	X			
AC-18(1)	Wireless Access Authentication and Encryption	+	X	X	+	X	X			
AC-18(2)	<i>Wireless Access Monitoring Unauthorized Connections</i>	Withdrawn								
AC-18(3)	Wireless Access Disable Wireless Networking	+	+	+	+	+	+			
AC-18(4)	Wireless Access Restrict Configurations by Users	+	+	X	+	+	X			
AC-18(5)	Wireless Access Antennas / Transmission Power Levels			X			X			
AC-19	Access Control For Mobile Devices	X	X	X	X	X	X			
AC-19(1)	<i>Access Control For Mobile Devices Use of Writable / Portable Storage Devices</i>	Withdrawn								
AC-19(2)	<i>Access Control For Mobile Devices Use of Personally Owned Portable Storage Devices</i>	Withdrawn								
AC-19(3)	<i>Access Control For Mobile Devices Use of Portable Storage Devices with No Identifiable Owner</i>	Withdrawn								
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		X	X			
AC-20	Use of External Information Systems	X	X	X	X	X	X			
AC-20(1)	Use of External Information Systems Limits on Authorized Use	+	X	X	+	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									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
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									
AT-1	Security Awareness and Training Policy and Procedures	X	X	X	X	X	X	X	X	X
AT-2	Security Awareness Training	X	X	X	X	X	X	X	X	X
AT-2(1)	Security Awareness Practical Exercises									
AT-2(2)	Security Awareness Insider Threat	+	X	X	+	X	X	+	X	X
AT-3	Role-Based Security Training	X	X	X	X	X	X	X	X	X
AT-3(1)	Security Training Environmental Controls									
AT-3(2)	Security Training Physical Security Controls	+	+	+	+	+	+	+	+	+
AT-3(3)	Security Training Practical Exercises									
AT-3(4)	Security Training Suspicious Communications and Anomalous System Behavior	+	+	+	+	+	+	+	+	+
AT-4	Security Training Records	X	X	X	X	X	X	X	X	X
AT-5	Contacts With Security Groups and Associations	Withdrawn								
AU-1	Audit and Accountability Policy and Procedures	X	X	X	X	X	X	X	X	X
AU-2	Audit Events	X	X	X	X	X	X			
AU-2(1)	Audit Events Compilation of Audit Records From Multiple Sources	Withdrawn								
AU-2(2)	Audit Events Selection of Audit Events by Component	Withdrawn								
AU-2(3)	Audit Events Reviews and Updates	+	X	X	+	X	X			
AU-2(4)	Audit Events Privileged Functions	Withdrawn								
AU-3	Content of Audit Records	X	X	X	X	X	X			
AU-3(1)	Content of Audit Records Additional Audit Information	+	X	X	+	X	X			
AU-3(2)	Content of Audit Records Centralized Management of Planned Audit Record Content			X			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-									X

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
	Time Alerts									
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	X	X			
AU-6(1)	Audit Review, Analysis, and Reporting Process Integration	+	X	X	+	X	X			
AU-6(2)	Audit Review, Analysis, and Reporting Automated Security Alerts	Withdrawn								
AU-6(3)	Audit Review, Analysis, and Reporting Correlate Audit Repositories	+	X	X	+	X	X			
AU-6(4)	Audit Review, Analysis, and Reporting Central Review and Analysis	+	+	+	+	+	+			
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									
AU-6(8)	Audit Review, Analysis, and Reporting Full Text Analysis of Privileged Commands									
AU-6(9)	Audit Review, Analysis, and Reporting Correlation with Information from Nontechnical Sources									
AU-6(10)	Audit Review, Analysis, and Reporting Audit Level Adjustment	+	+	+	+	+	+			
AU-7	Audit Reduction and Report Generation		X	X		X	X			
AU-7(1)	Audit Reduction and Report Generation Automatic Processing		X	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									
AU-9	Protection of Audit Information	X	X	X	X	X	X	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	+	X	X			

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AU-9(5)	Protection of Audit Information Dual Authorization									
AU-9(6)	Protection of Audit Information Read Only Access									
AU-10	Non-Repudiation					+	X			
AU-10(1)	Non-Repudiation Association of Identities									
AU-10(2)	Non-Repudiation Validate Binding of Information Producer Identity									
AU-10(3)	Non-Repudiation Chain of Custody									
AU-10(4)	Non-Repudiation Validate Binding of Information Reviewer Identity									
AU-10(5)	Non-Repudiation / Digital Signatures	Withdrawn								
AU-11	Audit Record Retention							X	X	X
AU-11(1)	Audit Record Retention Long-Term Retrieval Capability							+	+	+
AU-12	Audit Generation	X	X	X	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	+	+	X			
AU-13	Monitoring For Information Disclosure									
AU-13(1)	Monitoring For Information Disclosure Use of Automated Tools									
AU-13(2)	Monitoring For Information Disclosure Review of Monitored Sites									
AU-14	Session Audit	+	+	+	+	+	+			
AU-14(1)	Session Audit System Start-Up	+	+	+	+	+	+			
AU-14(2)	Session Audit Capture/Record and Log Content	+	+	+	+	+	+			
AU-14(3)	Session Audit Remote Viewing / Listening	+	+	+						
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									
CA-1	Security Assessment and Authorization Policies and Procedures	X	X	X	X	X	X	X	X	X
CA-2	Security Assessments	X	X	X	X	X	X	X	X	X
CA-2(1)	Security Assessments Independent Assessors	+	X	X	+	X	X	+	X	X
CA-2(2)	Security Assessments Specialized Assessments			X			X			X
CA-2(3)	Security Assessments External Organizations									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
CA-3	System Interconnections	X	X	X	X	X	X			
CA-3(1)	System Interconnections Unclassified National Security System Connections	+	+	+						
CA-3(2)	System Interconnections Classified National Security System Connections									
CA-3(3)	System Interconnections Unclassified Non-National Security System Connections									
CA-3(4)	System Interconnections Connections to Public Networks									
CA-3(5)	System Interconnections Restrictions on External Network Connections	+	X	X	+	X	X			
CA-4	Security Certification	Withdrawn								
CA-5	Plan of Action and Milestones	X	X	X	X	X	X	X	X	X
CA-5(1)	Plan of Action and Milestones Automation Support For Accuracy / Currency									
CA-6	Security Authorization	X	X	X	X	X	X	X	X	X
CA-7	Continuous Monitoring	X	X	X	X	X	X	X	X	X
CA-7(1)	Continuous Monitoring Independent Assessment		X	X		X	X		X	X
CA-7(2)	Continuous Monitoring Types of Assessments	Withdrawn								
CA-7(3)	Continuous Monitoring Trend Analyses									
CA-8	Penetration Testing						X			
CA-8(1)	Penetration Testing Independent Penetration Agent or Team									
CA-8(2)	Penetration Testing Red Team Exercises									
CA-9	Internal System Connections	X	X	X	X	X	X			
CA-9(1)	Internal System Connections Security Compliance Checks									
CM-1	Configuration Management Policy and Procedures	X	X	X	X	X	X			
CM-2	Baseline Configuration				X	X	X			
CM-2(1)	Baseline Configuration Reviews and Updates				+	X	X			
CM-2(2)	Baseline Configuration Automation Support For Accuracy / Currency						X			
CM-2(3)	Baseline Configuration Retention of Previous Configurations					X	X			
CM-2(4)	Baseline Configuration Unauthorized Software	Withdrawn								
CM-2(5)	Baseline Configuration Authorized Software	Withdrawn								
CM-2(6)	Baseline Configuration Development and Test Environments									
CM-2(7)	Baseline Configuration Configure Systems, Components, or Devices for High-Risk Areas					X	X			
CM-3	Configuration Change Control				+	X	X			

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
CM-3(1)	Configuration Change Control Automated Document / Notification / Prohibition of Changes						X			
CM-3(2)	Configuration Change Control Test / Validate / Document Changes					X	X			
CM-3(3)	Configuration Change Control Automated Change Implementation									
CM-3(4)	Configuration Change Control Security Representative				+	+	+			
CM-3(5)	Configuration Change Control Automated Security Response						+			
CM-3(6)	Configuration Change Control Cryptography Management				+	+	+			
CM-4	Security Impact Analysis				X	X	X			
CM-4(1)	Security Impact Analysis Separate Test Environments					+	X			
CM-4(2)	Security Impact Analysis Verification of Security Functions									
CM-5	Access Restrictions For Change				+	X	X			
CM-5(1)	Access Restrictions For Change Automated Access Enforcement / Auditing					+	X			
CM-5(2)	Access Restrictions For Change Review System Changes					+	X			
CM-5(3)	Access Restrictions For Change Signed Components						X			
CM-5(4)	Access Restrictions For Change Dual Authorization									
CM-5(5)	Access Restrictions For Change Limit Production / Operational Privileges				+	+	+			
CM-5(6)	Access Restrictions For Change Limit Library Privileges				+	+	+			
CM-5(7)	Access Restrictions For Change Automatic Implementation of Security Safeguards	Withdrawn								
CM-6	Configuration Settings				X	X	X			
CM-6(1)	Configuration Settings Automated Central Management / Application / Verification					+	X			
CM-6(2)	Configuration Settings Respond to Unauthorized Changes						X			
CM-6(3)	Configuration Settings Unauthorized Change Detection	Withdrawn								
CM-6(4)	Configuration Settings Conformance Demonstration	Withdrawn								
CM-7	Least Functionality	X	X	X	X	X	X			
CM-7(1)	Least Functionality Periodic Review	+	X	X	+	X	X			
CM-7(2)	Least Functionality Prevent Program Execution	+	X	X	+	X	X			
CM-7(3)	Least Functionality Registration Compliance	+	+	+	+	+	+			
CM-7(4)	Least Functionality Unauthorized Software /									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
	Blacklisting									
CM-7(5)	Least Functionality Authorized Software / Whitelisting	+	+	X	+	+	X			
CM-8	Information System Component Inventory				X	X	X			
CM-8(1)	Information System Component Inventory Updates During Installations / Removals					X	X			
CM-8(2)	Information System Component Inventory Automated Maintenance				+	+	X			
CM-8(3)	Information System Component Inventory Automated Unauthorized Component Detection				+	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			
CM-8(6)	Information System Component Inventory Assessed Configurations / Approved Deviations									
CM-8(7)	Information System Component Inventory Centralized Repository									
CM-8(8)	Information System Component Inventory Automated Location Tracking									
CM-8(9)	Information System Component Inventory Assignment of Components to Systems									
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	X	X	X			
CM-11(1)	User-Installed Software Alerts For Unauthorized Installations			+			+			
CM-11(2)	User-Installed Software Prohibit Installation without Privileged Status	+	+	+	+	+	+			
CP-1	Contingency Planning Policy and Procedures	X	X	X	X	X	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 /									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
	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
CP-3(1)	Contingency Training Simulated Events									X
CP-3(2)	Contingency Training Automated Training Environments									
CP-4	Contingency Plan Testing							X	X	X
CP-4(1)	Contingency Plan Testing Coordinate With Related Plans								X	X
CP-4(2)	Contingency Plan Testing Alternate Processing Site									X
CP-4(3)	Contingency Plan Testing Automated Testing									
CP-4(4)	Contingency Plan Testing Full Recovery / Reconstitution									
CP-5	Contingency Plan Update	Withdrawn								
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		X	X		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	Withdrawn								
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	X	X	X	X	X	X

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
CP-9(1)	Information System Backup Testing For Reliability / Integrity					X	X		X	X
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)	<i>Information System Backup / Protection From Unauthorized Modification</i>	Withdrawn								
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)	<i>Information System Recovery and Reconstitution / Contingency Plan Testing</i>	Withdrawn								
CP-10(2)	Information System Recovery and Reconstitution Transaction Recovery					X	X		X	X
CP-10(3)	<i>Information System Recovery and Reconstitution / Compensating Security Controls</i>	Withdrawn								
CP-10(4)	Information System Recovery and Reconstitution Restore Within Time Period						X			X
CP-10(5)	<i>Information System Recovery and Reconstitution / Failover Capability</i>	Withdrawn								
CP-10(6)	Information System Recovery and Reconstitution Component Protection									
CP-11	Alternate Communications Protocols									
CP-12	Safe Mode									
CP-13	Alternative Security Mechanisms									
IA-1	Identification and Authentication Policy and Procedures	X	X	X	X	X	X			
IA-2	Identification and Authentication (Organizational Users)	X	X	X	X	X	X			
IA-2(1)	Identification and Authentication (Organizational Users) Network Access to Privileged Accounts	X	X	X	X	X	X			
IA-2(2)	Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts	+	X	X	+	X	X			
IA-2(3)	Identification and Authentication (Organizational Users) Local Access to Privileged Accounts		X	X		X	X			
IA-2(4)	Identification and Authentication (Organizational Users) Local Access to Non-Privileged Accounts		+	X		+	X			

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
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	+	X	X			
IA-2(9)	Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts - Replay Resistant		+	X		+	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	+	X	X			
IA-2(12)	Identification and Authentication (Organizational Users) Acceptance of PIV Credentials	X	X	X	X	X	X			
IA-2(13)	Identification and Authentication Out-of-Band Authentication									
IA-3	Device Identification and Authentication	+	X	X	+	X	X			
IA-3(1)	Device Identification and Authentication Cryptographic Bidirectional Authentication		+	+		+	+			
IA-3(2)	<i>Device Identification and Authentication / Cryptographic Bidirectional Network Authentication</i>	<i>Withdrawn</i>								
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	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	X	X	X			

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
IA-5(1)	Authenticator Management Password-Based Authentication	X	X	X	X	X	X			
IA-5(2)	Authenticator Management PKI-Based Authentication		X	X		X	X			
IA-5(3)	Authenticator Management In Person or Trusted Third-Party Registration					X	X			
IA-5(4)	Authenticator Management Automated Support for Password Strength Determination	+	+	+	+	+	+			
IA-5(5)	Authenticator Management Change Authenticators Prior to Delivery									
IA-5(6)	Authenticator Management Protection of Authenticators									
IA-5(7)	Authenticator Management No Embedded Unencrypted Static Authenticators	+	+	+						
IA-5(8)	Authenticator Management Multiple Information System Accounts	+	+	+	+	+	+			
IA-5(9)	Authenticator Management Cross-Organization Credential Management									
IA-5(10)	Authenticator Management Dynamic Credential Association									
IA-5(11)	Authenticator Management Hardware Token-Based Authentication				X	X	X			
IA-5(12)	Authenticator Management Biometric Authentication									
IA-5(13)	Authenticator Management Expiration of Cached Authenticators	+	+	+	+	+	+			
IA-5(14)	Authenticator Management Managing Content of PKI Trust stores	+	+	+	+	+	+			
IA-5(15)	Authenticator Management FICAM-Approved Products and Services									
IA-6	Authenticator Feedback	X	X	X						
IA-7	Cryptographic Module Authentication	X	X	X	X	X	X			
IA-8	Identification and Authentication (Non-Organizational Users)	X	X	X	X	X	X			
IA-8(1)	Identification and Authentication (Non-Organizational Users) Acceptance of PIV Credentials from Other Agencies	X	X	X	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									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
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			+			+			
IR-1	Incident Response Policy and Procedures	X	X	X	X	X	X	X	X	X
IR-2	Incident Response Training	X	X	X	X	X	X	X	X	X
IR-2(1)	Incident Response Training Simulated Events			X			X			X
IR-2(2)	Incident Response Training Automated Training Environments						X			X
IR-3	Incident Response Testing	+	X	X	+	X	X	+	X	X
IR-3(1)	Incident Response Testing Automated Testing									
IR-3(2)	Incident Response Testing Coordination With Related Plans		X	X		X	X		X	X
IR-4	Incident Handling	X	X	X	X	X	X	X	X	X
IR-4(1)	Incident Handling Automated Incident Handling Processes		X	X		X	X		X	X
IR-4(2)	Incident Handling Dynamic Reconfiguration									
IR-4(3)	Incident Handling Continuity of Operations		+	+		+	+		+	+
IR-4(4)	Incident Handling Information Correlation	+	+	X	+	+	X	+	+	X
IR-4(5)	Incident Handling Automatic Disabling of Information System									
IR-4(6)	Incident Handling Insider Threats - Specific Capabilities	+	+	+	+	+	+	+	+	+
IR-4(7)	Incident Handling Insider Threats - Intra-Organization Coordination	+	+	+	+	+	+	+	+	+
IR-4(8)	Incident Handling Correlation With External Organizations	+	+	+	+	+	+	+	+	+
IR-4(9)	Incident Handling Dynamic Response Capability									
IR-4(10)	Incident Handling Supply Chain Coordination									
IR-5	Incident Monitoring	X	X	X	X	X	X	X	X	X
IR-5(1)	Incident Monitoring Automated Tracking / Data Collection / Analysis			X			X			X
IR-6	Incident Reporting	X	X	X	X	X	X	X	X	X
IR-6(1)	Incident Reporting Automated Reporting		X	X		X	X		X	X
IR-6(2)	Incident Reporting Vulnerabilities Related to Incidents	+	+	+	+	+	+	+	+	+
IR-6(3)	Incident Reporting Coordination With Supply Chain									
IR-7	Incident Response Assistance	X	X	X	X	X	X	X	X	X

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
IR-7(1)	Incident Response Assistance Automation Support For Availability of Information / Support		X	X		X	X		X	X
IR-7(2)	Incident Response Assistance Coordination With External Providers	+	+	+	+	+	+	+	+	+
IR-8	Incident Response Plan	X	X	X	X	X	X	X	X	X
IR-9	Information Spillage Response	+	+	+						
IR-9(1)	Information Spillage Response Responsible Personnel	+	+	+						
IR-9(2)	Information Spillage Response Training	+	+	+						
IR-9(3)	Information Spillage Response Post-Spill Operations								+	+
IR-9(4)	Information Spillage Response Exposure to Unauthorized Personnel	+	+	+						
IR-10	Integrated Information Security Cell		+	+		+	+		+	+
MA-1	System Maintenance Policy and Procedures	X	X	X	X	X	X	X	X	X
MA-2	Controlled Maintenance	X	X	X	X	X	X	X	X	X
MA-2(1)	<i>Controlled Maintenance / Record Content</i>	<i>Withdrawn</i>								
MA-2(2)	Controlled Maintenance Automated Maintenance Activities			X			X			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	+	+	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	X	X	X	X	X	X
MA-5(1)	Maintenance Personnel Individuals Without Appropriate Access			X			X			X
MA-5(2)	Maintenance Personnel Security Clearances For Classified Systems									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
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									
MP-1	Media Protection Policy and Procedures	X	X	X	X	X	X			
MP-2	Media Access	X	X	X	X	X	X			
MP-2(1)	Media Access Automated Restricted Access	Withdrawn								
MP-2(2)	Media Access Cryptographic Protection	Withdrawn								
MP-3	Media Marking		X	X						
MP-4	Media Storage		X	X		X	X			
MP-4(1)	Media Storage Cryptographic Protection	Withdrawn								
MP-4(2)	Media Storage Automated Restricted Access									
MP-5	Media Transport		X	X		X	X			
MP-5(1)	Media Transport Protection Outside of Controlled Areas	Withdrawn								
MP-5(2)	Media Transport Documentation of Activities	Withdrawn								
MP-5(3)	Media Transport Custodians									
MP-5(4)	Media Transport Cryptographic Protection		X	X		X	X			
MP-6	Media Sanitization	X	X	X						
MP-6(1)	Media Sanitization Review / Approve / Track / Document / Verify			X						
MP-6(2)	Media Sanitization Equipment Testing			X						
MP-6(3)	Media Sanitization Nondestructive Techniques			X						
MP-6(4)	Media Sanitization Controlled Unclassified Information	Withdrawn								
MP-6(5)	Media Sanitization Classified Information	Withdrawn								
MP-6(6)	Media Sanitization Media Destruction	Withdrawn								
MP-6(7)	Media Sanitization Dual Authorization									
MP-6(8)	Media Sanitization Remote Purging / Wiping of Information									
MP-7	Media Use	X	X	X	X	X	X			
MP-7(1)	Media Use Prohibit Use without Owner				+	X	X			
MP-7(2)	Media Use Prohibit Use of Sanitization-Resistant Media									
MP-8	Media Downgrading									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
MP-8(1)	Media Downgrading Documentation of Process									
MP-8(2)	Media Downgrading Equipment Testing									
MP-8(3)	Media Downgrading Controlled Unclassified Information									
MP-8(4)	Media Downgrading Classified Information									
PE-1	Physical and Environmental Protection Policy and Procedures	X	X	X	X	X	X	X	X	X
PE-2	Physical Access Authorizations	X	X	X	X	X	X	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	X	X	X	X	X	X
PE-3(1)	Physical Access Control Information System Access	+	+	X	+	+	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		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	X	X	X	X	X
PE-6(1)	Monitoring Physical Access Intrusion Alarms / Surveillance Equipment		X	X		X	X		X	X
PE-6(2)	Monitoring Physical Access Automated Intrusion Recognition / Responses									
PE-6(3)	Monitoring Physical Access Video Surveillance									
PE-6(4)	Monitoring Physical Access Monitoring Physical Access to Information Systems			X			X			X
PE-7	Visitor Control	Withdrawn								
PE-7(1)	Visitor Control	Withdrawn								
PE-7(2)	Visitor Control	Withdrawn								

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
PE-8	Visitor Access Records	X	X	X	X	X	X	X	X	X
PE-8(1)	Visitor Access Records Automated Records Maintenance / Review			X			X			
PE-8(2)	Visitor Access Records / Physical Access Records	Withdrawn								
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	Withdrawn								
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									
PE-12	Emergency Lighting							X	X	X
PE-12(1)	Emergency Lighting Essential Missions / Business Functions									
PE-13	Fire Protection							X	X	X
PE-13(1)	Fire Protection Detection Devices / Systems									X
PE-13(2)	Fire Protection Suppression Devices / Systems									X
PE-13(3)	Fire Protection Automatic Fire Suppression								X	X
PE-13(4)	Fire Protection Inspections									+
PE-14	Temperature and Humidity Controls							X	X	X
PE-14(1)	Temperature and Humidity Controls Automatic Controls									
PE-14(2)	Temperature and Humidity Controls Monitoring With Alarms / Notifications									
PE-15	Water Damage Protection							X	X	X
PE-15(1)	Water Damage Protection Automation Support									X
PE-16	Delivery and Removal	X	X	X	X	X	X	X	X	X
PE-17	Alternate Work Site		X	X		X	X		X	X
PE-18	Location of Information System Components									X
PE-18(1)	Location of Information System Components Facility Site									
PE-19	Information Leakage									
PE-19(1)	Information Leakage National Emissions / TEMPEST Policies and Procedures									
PE-20	Asset Monitoring and Tracking									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
PL-1	Security Planning Policy and Procedures	X	X	X	X	X	X	X	X	X
PL-2	System Security Plan	X	X	X	X	X	X	X	X	X
PL-2(1)	System Security Plan / Concept of Operations	Withdrawn								
PL-2(2)	System Security Plan / Functional Architecture	Withdrawn								
PL-2(3)	System Security Plan Plan / Coordinate With Other Organizational Entities		X	X		X	X		X	X
PL-3	System Security Plan Update	Withdrawn								
PL-4	Rules of Behavior	X	X	X	X	X	X	X	X	X
PL-4(1)	Rules of Behavior Social Media and Networking Restrictions		X	X						
PL-5	Privacy Impact Assessment	Withdrawn								
PL-6	Security-Related Activity Planning	Withdrawn								
PL-7	Security Concept of Operations									
PL-8	Information Security Architecture	+	X	X	+	X	X	+	X	X
PL-8(1)	Information Security Architecture Defense-in-Depth	+	+	+	+	+	+	+	+	+
PL-8(2)	Information Security Architecture Supplier Diversity	+	+	+	+	+	+	+	+	+
PL-9	Central Management									
PS-1	Personnel Security Policy and Procedures	X	X	X	X	X	X	X	X	X
PS-2	Position Risk Designation	X	X	X	X	X	X	X	X	X
PS-3	Personnel Screening	X	X	X	X	X	X			
PS-3(1)	Personnel Screening Classified Information									
PS-3(2)	Personnel Screening Formal Indoctrination									
PS-3(3)	Personnel Screening Information With Special Protection Measures									
PS-4	Personnel Termination	X	X	X	X	X	X	X	X	X
PS-4(1)	Personnel Termination Post-Employment Requirements	+	+	+						
PS-4(2)	Personnel Termination Automated Notification			X			X			X
PS-5	Personnel Transfer	X	X	X	X	X	X	X	X	X
PS-6	Access Agreements	X	X	X	X	X	X			
PS-6(1)	Access Agreements / Information Requiring Special Protection	Withdrawn								
PS-6(2)	Access Agreements Classified Information Requiring Special Protection									
PS-6(3)	Access Agreements Post-Employment Requirements	+	+	+						
PS-7	Third-Party Personnel Security	X	X	X	X	X	X			
PS-8	Personnel Sanctions	X	X	X	X	X	X	X	X	X
RA-1	Risk Assessment Policy and Procedures	X	X	X	X	X	X	X	X	X
RA-2	Security Categorization	X	X	X	X	X	X	X	X	X

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
RA-3	Risk Assessment	X	X	X	X	X	X	X	X	X
RA-4	<i>Risk Assessment Update</i>	<i>Withdrawn</i>								
RA-5	Vulnerability Scanning	X	X	X	X	X	X	X	X	X
RA-5(1)	Vulnerability Scanning Update Tool Capability	+	X	X	+	X	X	+	X	X
RA-5(2)	Vulnerability Scanning Update by Frequency / Prior to New Scan / When Identified	+	X	X	+	X	X	+	X	X
RA-5(3)	Vulnerability Scanning Breadth /Depth of Coverage									
RA-5(4)	Vulnerability Scanning Discoverable Information	+	+	X	+	+	X	+	+	X
RA-5(5)	Vulnerability Scanning Privileged Access	+	X	X	+	X	X	+	X	X
RA-5(6)	Vulnerability Scanning Automated Trend Analyses									
RA-5(7)	<i>Vulnerability Scanning / Automated Detection and Notification of Unauthorized Components</i>	<i>Withdrawn</i>								
RA-5(8)	Vulnerability Scanning Review Historic Audit Logs									
RA-5(9)	<i>Vulnerability Scanning / Penetration Testing and Analyses</i>	<i>Withdrawn</i>								
RA-5(10)	Vulnerability Scanning Correlate Scanning Information			+			+			+
RA-6	Technical Surveillance Countermeasures Survey									
SA-1	System and Services Acquisition Policy and Procedures	X	X	X	X	X	X	X	X	X
SA-2	Allocation of Resources	X	X	X	X	X	X	X	X	X
SA-3	System Development Life Cycle	X	X	X	X	X	X	X	X	X
SA-4	Acquisition Process	X	X	X	X	X	X	X	X	X
SA-4(1)	Acquisition Process Functional Properties of Security Controls		X	X		X	X		X	X
SA-4(2)	Acquisition Process Design / Implementation Information for Security Controls		X	X		X	X		X	X
SA-4(3)	Acquisition Process Development Methods / Techniques / Practices						+			
SA-4(4)	<i>Acquisition Process / Assignment of Components to Systems</i>	<i>Withdrawn</i>								
SA-4(5)	Acquisition Process System / Component / Service Configurations						+			
SA-4(6)	Acquisition Process Use of Information Assurance Products									
SA-4(7)	Acquisition Process NIAP-Approved Protection Profiles				+	+	+			
SA-4(8)	Acquisition Process Continuous Monitoring Plan									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
SA-4(9)	Acquisition Process Functions / Ports / Protocols / Services in Use	+	X	X	+	X	X	+	X	X
SA-4(10)	Acquisition Process Use of Approved PIV Products	X	X	X	X	X	X			
SA-5	Information System Documentation	X	X	X	X	X	X	X	X	X
SA-5(1)	Information System Documentation / Functional Properties of Security Controls	Withdrawn								
SA-5(2)	Information System Documentation / Security-Relevant External System Interfaces	Withdrawn								
SA-5(3)	Information System Documentation / High-Level Design	Withdrawn								
SA-5(4)	Information System Documentation / Low-Level Design	Withdrawn								
SA-5(5)	Information System Documentation / Source Code	Withdrawn								
SA-6	Software Usage Restrictions	Withdrawn								
SA-6(1)	Software Usage Restrictions	Withdrawn								
SA-7	User-Installed Software	Withdrawn								
SA-8	Security Engineering Principles	+	X	X	+	X	X	+	X	X
SA-9	External Information System Services	X	X	X	X	X	X	X	X	X
SA-9(1)	External Information Systems Risk Assessments / Organizational Approvals				+	+	+			
SA-9(2)	External Information Systems Identification of Functions / Ports / Protocols / Services	+	X	X	+	X	X	+	X	X
SA-9(3)	External Information Systems Establish / Maintain Trust Relationship with Providers									
SA-9(4)	External Information Systems Consistent Interests of Consumers and Providers									
SA-9(5)	External Information Systems Processing, Storage, and Service Location									
SA-10	Developer Configuration Management				+	X	X			
SA-10(1)	Developer Configuration Management Software / Firmware Integrity Verification				+	+	+			
SA-10(2)	Developer Configuration Management Alternative Configuration Management Processes									
SA-10(3)	Developer Configuration Management Hardware Integrity Verification									
SA-10(4)	Developer Configuration Management Trusted Generation									
SA-10(5)	Developer Configuration Management Mapping Integrity for Version Control									
SA-10(6)	Developer Configuration Management Trusted Distribution									
SA-11	Developer Security Testing and Evaluation		X	X		X	X		X	X

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
SA-11(1)	Developer Security Testing and Evaluation Static Code Analysis									
SA-11(2)	Developer Security Testing and Evaluation Threat and Vulnerability Analyses									
SA-11(3)	Developer Security Testing and Evaluation Independent Verification of Assessment Plans / Evidence									
SA-11(4)	Developer Security Testing and Evaluation Manual Code Reviews									
SA-11(5)	Developer Security Testing and Evaluation Penetration Testing / Analysis									
SA-11(6)	Developer Security Testing and Evaluation Attack Surface Reviews									
SA-11(7)	Developer Security Testing and Evaluation Verify Scope of Testing / Evaluation									
SA-11(8)	Developer Security Testing and Evaluation Dynamic Code Analysis									
SA-12	Supply Chain Protection	+	+	X	+	+	X	+	+	X
SA-12(1)	Supply Chain Protection Acquisition Strategies / Tools / Methods			+			+			+
SA-12(2)	Supply Chain Protection Supplier Reviews									
SA-12(3)	Supply Chain Protection Trusted Shipping and Warehousing	Withdrawn								
SA-12(4)	Supply Chain Protection Diversity of Suppliers	Withdrawn								
SA-12(5)	Supply Chain Protection Limitation of Harm			+			+			+
SA-12(6)	Supply Chain Protection Minimizing Procurement Time	Withdrawn								
SA-12(7)	Supply Chain Protection Assessments Prior to Selection / Acceptance / Update									
SA-12(8)	Supply Chain Protection Use of All-Source Intelligence			+			+			+
SA-12(9)	Supply Chain Protection Operations Security			+			+			+
SA-12(10)	Supply Chain Protection Validate As Genuine and Not Altered									
SA-12(11)	Supply Chain Protection Penetration Testing / Analysis of Elements, Processes, and Actors			+			+			+
SA-12(12)	Supply Chain Protection Inter-Organizational Agreements									
SA-12(13)	Supply Chain Protection Critical Information System Components									
SA-12(14)	Supply Chain Protection Identity and Traceability									
SA-12(15)	Supply Chain Protection Processes to Address Weaknesses or Deficiencies									
SA-13	Trustworthiness									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
SA-14	Criticality Analysis			+			+			+
SA-14(1)	<i>Criticality Analysis / Critical Components with No Viable Alternative Sourcing</i>	Withdrawn								
SA-15	Development Process, Standards, and Tools	+	+	X	+	+	X	+	+	X
SA-15(1)	Development Process, Standards, and Tools Quality Metrics									
SA-15(2)	Development Process, Standards, and Tools Security Tracking Tools									
SA-15(3)	Development Process, Standards, and Tools Criticality Analysis			+			+			+
SA-15(4)	Development Process, Standards, and Tools Threat Modeling / Vulnerability Analysis			+			+			+
SA-15(5)	Development Process, Standards, and Tools Attack Surface Reduction									
SA-15(6)	Development Process, Standards, and Tools Continuous Improvement									
SA-15(7)	Development Process, Standards, and Tools Automated Vulnerability Analysis						+			
SA-15(8)	Development Process, Standards, and Tools Reuse of Threat / Vulnerability Information									
SA-15(9)	Development Process, Standards, and Tools Use of Live Data	+	+	+						
SA-15(10)	Development Process, Standards, and Tools Incident Response Plan									
SA-15(11)	Development Process, Standards, and Tools Archive Information System / Component									
SA-16	Developer-Provided Training			X			X			X
SA-17	Developer Security Architecture and Design			X			X			X
SA-17(1)	Developer Security Architecture and Design Formal Policy Model									
SA-17(2)	Developer Security Architecture and Design Security-Relevant Components									
SA-17(3)	Developer Security Architecture and Design Formal Correspondence									
SA-17(4)	Developer Security Architecture and Design Informal Correspondence									
SA-17(5)	Developer Security Architecture and Design Conceptually Simple Design									
SA-17(6)	Developer Security Architecture and Design Structure for Testing									
SA-17(7)	Developer Security Architecture and Design Structure for Least Privilege									
SA-18	Tamper Resistance and Detection									
SA-18(1)	Tamper Resistance and Detection Multiple Phases of SDLC									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
SA-18(2)	Tamper Resistance and Detection Inspection of Information Systems, Components, or Devices									
SA-19	Component Authenticity				+	+	+			
SA-19(1)	Component Authenticity Anti-Counterfeit Training									
SA-19(2)	Component Authenticity Configuration Control for Component Service / Repair									
SA-19(3)	Component Authenticity Component Disposal									
SA-19(4)	Component Authenticity Anti-Counterfeit Scanning									
SA-20	Customized Development of Critical Components									
SA-21	Developer Screening									
SA-21(1)	Developer Screening Validation of Screening									
SA-22	Unsupported System Components			+			+			+
SA-22(1)	Unsupported System Components Alternative Sources for Continued Support									
SC-1	System and Communications Protection Policy and Procedures	X	X	X	X	X	X	X	X	X
SC-2	Application Partitioning		X	X		X	X			
SC-2(1)	Application Partitioning Interfaces For Non-Privileged Users									
SC-3	Security Function Isolation			X			X			
SC-3(1)	Security Function Isolation Hardware Separation									
SC-3(2)	Security Function Isolation Access / Flow Control Functions									
SC-3(3)	Security Function Isolation Minimize Nonsecurity Functionality									
SC-3(4)	Security Function Isolation Module Coupling and Cohesiveness									
SC-3(5)	Security Function Isolation Layered Structures									
SC-4	Information In Shared Resources		X	X						
SC-4(1)	Information In Shared Resources / Security Levels	Withdrawn								
SC-4(2)	Information In Shared Resources Periods Processing									
SC-5	Denial of Service Protection							X	X	X
SC-5(1)	Denial of Service Protection Restrict Internal Users							+	+	+
SC-5(2)	Denial of Service Protection Excess Capacity / Bandwidth / Redundancy								+	+
SC-5(3)	Denial of Service Protection Detection / Monitoring								+	+

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
SC-6	Resource Availability									
SC-7	Boundary Protection	X	X	X	X	X	X			
SC-7(1)	Boundary Protection / Physically Separated Subnetworks	Withdrawn								
SC-7(2)	Boundary Protection / Public Access	Withdrawn								
SC-7(3)	Boundary Protection Access Points	+	X	X	+	X	X			
SC-7(4)	Boundary Protection External Telecommunications Services	+	X	X	+	X	X			
SC-7(5)	Boundary Protection Deny by Default / Allow by Exception	+	X	X	+	X	X			
SC-7(6)	Boundary Protection / Response to Recognized Failures	Withdrawn								
SC-7(7)	Boundary Protection Prevent Split Tunneling for Remote Devices	+	X	X	+	X	X			
SC-7(8)	Boundary Protection Route Traffic to Authenticated Proxy Servers	+	+	X	+	+	X			
SC-7(9)	Boundary Protection Restrict Threatening Outgoing Communications Traffic				+	+	+			
SC-7(10)	Boundary Protection Prevent Unauthorized Exfiltration	+	+	+						
SC-7(11)	Boundary Protection Restrict Incoming Communications Traffic				+	+	+			
SC-7(12)	Boundary Protection Host-Based Protection	+	+	+	+	+	+	+	+	+
SC-7(13)	Boundary Protection Isolation of Security Tools / Mechanisms / Support Components	+	+	+	+	+	+			
SC-7(14)	Boundary Protection Protect Against Unauthorized Physical Connections	+	+	+	+	+	+			
SC-7(15)	Boundary Protection Route Privileged Network Accesses									
SC-7(16)	Boundary Protection Prevent Discovery of Components / Devices									
SC-7(17)	Boundary Protection Automated Enforcement of Protocol Formats									
SC-7(18)	Boundary Protection Fail Secure			X			X			X
SC-7(19)	Boundary Protection Block 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									
SC-7(23)	Boundary Protection Disable Sender Feedback on Protocol Validation Failure									
SC-8	Transmission Confidentiality and Integrity	+	X	X	+	X	X			
SC-8(1)	Transmission Confidentiality and Integrity Cryptographic or Alternate Physical	+	X	X	+	X	X			

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
	Protection									
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	Withdrawn								
SC-9(1)	Transmission Confidentiality Cryptographic or Alternate Physical Protection	Withdrawn								
SC-9(2)	Transmission Confidentiality Pre / Post Transmission Handling	Withdrawn								
SC-10	Network Disconnect		X	X		X	X			
SC-11	Trusted Path									
SC-11(1)	Trusted Path Logical Isolation									
SC-12	Cryptographic Key Establishment and Management	X	X	X	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	Withdrawn								
SC-12(5)	Cryptographic Key Establishment and Management PKI Certificates / Hardware Tokens	Withdrawn								
SC-13	Cryptographic Protection	X	X	X	X	X	X			
SC-13(1)	Cryptographic Protection FIPS-Validated Cryptography	Withdrawn								
SC-13(2)	Cryptographic Protection NSA-Approved Cryptography	Withdrawn								
SC-13(3)	Cryptographic Protection Individuals Without Formal Access Approvals	Withdrawn								
SC-13(4)	Cryptographic Protection Digital Signatures	Withdrawn								
SC-14	Public Access Protections	Withdrawn								
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	Withdrawn								
SC-15(3)	Collaborative Computing Devices Disabling / Removal In Secure Work Areas									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
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	+	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	+	X	X	+	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	Withdrawn								
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	Withdrawn								
SC-22	Architecture and Provisioning for Name / Address Resolution Service	X	X	X	X	X	X	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	Withdrawn								
SC-23(3)	Session Authenticity Unique Session Identifiers With Randomization				+	+	+			
SC-23(4)	Session Authenticity Unique Session Identifiers With Randomization	Withdrawn								
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	Withdrawn								

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
SC-27	Platform-Independent Applications									
SC-28	Protection of Information At Rest	+	X	X	+	X	X			
SC-28(1)	Protection of Information At Rest Cryptographic Protection	+	+	+	+	+	+			
SC-28(2)	Protection of Information At Rest Off-Line Storage									
SC-29	Heterogeneity									
SC-29(1)	Heterogeneity Virtualization Techniques									
SC-30	Concealment and Misdirection									
SC-30(1)	<i>Concealment and Misdirection / Virtualization Techniques</i>	<i>Withdrawn</i>								
SC-30(2)	Concealment and Misdirection Randomness									
SC-30(3)	Concealment and Misdirection Change Processing / Storage Locations									
SC-30(4)	Concealment and Misdirection Misleading Information									
SC-30(5)	Concealment and Misdirection Concealment of System Components									
SC-31	Covert Channel Analysis									
SC-31(1)	Covert Channel Analysis Test Covert Channels for Exploitability									
SC-31(2)	Covert Channel Analysis Maximum Bandwidth									
SC-31(3)	Covert Channel Analysis Measure Bandwidth In Operational Environments									
SC-32	Information System Partitioning									
SC-33	<i>Transmission Preparation Integrity</i>	<i>Withdrawn</i>								
SC-34	Non-modifiable executable programs									
SC-34(1)	Non-Modifiable Executable Programs No Writable Storage									
SC-34(2)	Non-Modifiable Executable Programs Integrity Protection / Read-Only Media									
SC-34(3)	Non-Modifiable Executable Programs Hardware-Based Protection									
SC-35	Honeyclients									
SC-36	Distributed Processing and Storage									
SC-36(1)	Distributed Processing and Storage Polling Techniques									
SC-37	Out-of-Band Channels									
SC-37(1)	Out-Of-Band Channels Ensure Delivery / Transmission									
SC-38	Operations Security	+	+	+	+	+	+	+	+	+
SC-39	Process Isolation	X	X	X	X	X	X			
SC-39(1)	Process Isolation Hardware Separation									
SC-39(2)	Process Isolation Thread Isolation									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
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									
SI-1	System and Information Integrity Policy and Procedures	X	X	X	X	X	X	X	X	X
SI-2	Flaw Remediation				X	X	X			
SI-2(1)	Flaw Remediation Central Management				+	+	X			
SI-2(2)	Flaw Remediation Automated Flaw Remediation Status				+	X	X			
SI-2(3)	Flaw Remediation Time to Remediate Flaws / Benchmarks for Corrective Actions				+	+	+			
SI-2(4)	Flaw Remediation Automated Patch Management Tools	Withdrawn								
SI-2(5)	Flaw Remediation Automatic software / Firmware Updates									
SI-2(6)	Flaw Remediation Removal of Previous Versions of Software / Firmware				+	+	+			
SI-3	Malicious Code Protection				X	X	X			
SI-3(1)	Malicious Code Protection Central Management				+	X	X			
SI-3(2)	Malicious Code Protection Automatic Updates				+	X	X			
SI-3(3)	Malicious Code Protection Non-Privileged Users	Withdrawn								
SI-3(4)	Malicious Code Protection Updates Only by Privileged Users									
SI-3(5)	Malicious Code Protection Portable Storage Devices	Withdrawn								
SI-3(6)	Malicious Code Protection Testing / Verification									
SI-3(7)	Malicious Code Protection Non Signature-Based Detection									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
SI-3(8)	Malicious Code Protection Detect Unauthorized Commands									
SI-3(9)	Malicious Code Protection Authenticate Remote commands									
SI-3(10)	Malicious Code Protection Malicious Code Analysis				+	+	+			
SI-4	Information System Monitoring	X	X	X	X	X	X	X	X	X
SI-4(1)	Information System Monitoring System-Wide Intrusion Detection System	+	+	+	+	+	+	+	+	+
SI-4(2)	Information System Monitoring Automated Tools For Real-Time Analysis		X	X		X	X		X	X
SI-4(3)	Information System Monitoring Automated Tool Integration									
SI-4(4)	Information System Monitoring Inbound and Outbound Communications Traffic	+	X	X	+	X	X	+	X	X
SI-4(5)	Information System Monitoring System-Generated Alerts	+	X	X	+	X	X	+	X	X
SI-4(6)	Information System Monitoring Restrict Non-Privileged Users	Withdrawn								
SI-4(7)	Information System Monitoring Automated Response to Suspicious Events									
SI-4(8)	Information System Monitoring Protection of Monitoring Information	Withdrawn								
SI-4(9)	Information System Monitoring Testing of Monitoring Tools									
SI-4(10)	Information System Monitoring Visibility of Encrypted Communications		+	+		+	+		+	+
SI-4(11)	Information System Monitoring Analyze Communications Traffic Anomalies	+	+	+	+	+	+	+	+	+
SI-4(12)	Information System Monitoring Automated Alerts	+	+	+	+	+	+	+	+	+
SI-4(13)	Information System Monitoring Analyze Traffic / Event Patterns									
SI-4(14)	Information System Monitoring Wireless Intrusion Detection	+	+	+	+	+	+	+	+	+
SI-4(15)	Information System Monitoring Wireless to Wireline Communications	+	+	+	+	+	+	+	+	+
SI-4(16)	Information System Monitoring Correlate Monitoring Information	+	+	+	+	+	+	+	+	+
SI-4(17)	Information System Monitoring Integrated Situational Awareness									
SI-4(18)	Information System Monitoring Analyze Traffic / Covert Exfiltration									
SI-4(19)	Information System Monitoring Individuals Posing Greater Risk	+	+	+	+	+	+	+	+	+
SI-4(20)	Information System Monitoring Privileged User	+	+	+	+	+	+	+	+	+
SI-4(21)	Information System Monitoring									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
	Probationary Periods									
SI-4(22)	Information System Monitoring Unauthorized Network Services	+	+	+	+	+	+	+	+	+
SI-4(23)	Information System Monitoring Host-Based Devices	+	+	+	+	+	+	+	+	+
SI-4(24)	Information System Monitoring Indicators of Compromise									
SI-5	Security Alerts, Advisories, and Directives				X	X	X			
SI-5(1)	Security Alerts, Advisories, and Directives Automated Alerts and Advisories						X			
SI-6	Security Function Verification						X			
SI-6(1)	Security Function Verification Notification of Failed Security Tests	Withdrawn								
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			
SI-7(1)	Software, Firmware, and Information Integrity Integrity Checks					X	X			
SI-7(2)	Software, Firmware, and Information Integrity Automated Notifications of Integrity Violations						X			
SI-7(3)	Software, Firmware, and Information Integrity Centrally-Managed Integrity Tools									
SI-7(4)	Software, Firmware, and Information Integrity Tamper-Evident Packaging	Withdrawn								
SI-7(5)	Software, Firmware, and Information Integrity Automated Response to Integrity Violations						X			
SI-7(6)	Software, Firmware, and Information Integrity Cryptographic Protection									
SI-7(7)	Software, Firmware, and Information Integrity Integration of Detection and Response					X	X			
SI-7(8)	Software, Firmware, and Information Integrity Auditing Capability For Significant Events					+	+			
SI-7(9)	Software, Firmware, and Information Integrity Verify Boot Process									
SI-7(10)	Software, Firmware, and Information Integrity Protection of Boot Firmware									
SI-7(11)	Software, Firmware, and Information Integrity Confined Environments With Limited Privileges									
SI-7(12)	Software, Firmware, and Information Integrity Integrity Verification									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
SI-7(13)	Software, Firmware, and Information Integrity Code Execution In Protected Environments									
SI-7(14)	Software, Firmware, and Information Integrity Binary or Machine Executable Code				+	+	X			
SI-7(15)	Software, Firmware, and Information Integrity Code Authentication									
SI-7(16)	Software, Firmware, and Information Integrity Time Limit on Process Execution without Supervision									
SI-8	Spam Protection					X	X		X	X
SI-8(1)	Spam Protection Central Management of Protection Mechanisms					X	X		X	X
SI-8(2)	Spam Protection Automatic Updates					X	X		X	X
SI-8(3)	Spam Protection Continuous Learning Capability									
SI-9	Information Input Restrictions	Withdrawn								
SI-10	Information Input Validation				+	X	X			
SI-10(1)	Information Input Validation Manual Override Capability									
SI-10(2)	Information Input Validation Review / Resolution of Errors									
SI-10(3)	Information Input Validation Predictable Behavior					+	+			
SI-10(4)	Information Input Validation Review / Timing Interactions									
SI-10(5)	Information Input Validation Review / Restrict Inputs to Trusted Sources and Approved Formats									
SI-11	Error Handling				+	X	X			
SI-12	Information Handling and Retention	X	X	X	X	X	X			
SI-13	Predictable Failure Prevention									
SI-13(1)	Predictable Failure Prevention Transferring Component Responsibilities									
SI-13(2)	Predictable Failure Prevention / Time Limit on Process Execution without Supervision	Withdrawn								
SI-13(3)	Predictable Failure Prevention Manual Transfer between Components									
SI-13(4)	Predictable Failure Prevention Standby Component Installation / Notification									
SI-13(5)	Predictable Failure Prevention Failover Capability									
SI-14	Non-Persistence									
SI-14(1)	Non-Persistence Refresh from Trusted Sources									
SI-15	Information Output Filtering									

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
SI-16	Memory Protection					X	X			
SI-17	Fail-Safe Procedures									
PM-1	Information Security Program Plan	<p>Deployed organization-wide. Supporting information security program. Not associated with security control baselines. Independent of any impact level.</p>								
PM-2	Senior Information Security Officer									
PM-3	Information Security Resources									
PM-4	Plan of Action and Milestones Process									
PM-5	Information System Inventory									
PM-6	Information Security Measures of Performance									
PM-7	Enterprise Architecture									
PM-8	Critical Infrastructure Plan									
PM-9	Risk Management Strategy									
PM-10	Security Authorization Process									
PM-11	Mission/Business Process Definition									
PM-12	Insider Threat Program									
PM-13	Information Security Workforce									
PM-14	Testing, Training, and Monitoring									
PM-15	Contacts with Security Groups and Associations									
PM-16	Threat Awareness Program									

D.2 ADDITIONAL SECURITY CONTROL INFORMATION

Table D-2 includes additional information about the NIST SP 800-53 security controls, including confidentiality, integrity, and availability associations, justifications for inclusion in NSS baselines, and potentially common/inheritable controls.

Association of Confidentiality, Integrity, and Availability to NIST Security Controls: The security objectives of confidentiality, integrity, and availability are defined in 44 United States Code (U.S.C.), Section 3542. The NIST SP 800-53 control baselines do not characterize security controls as having relationships with security objectives. Table D-2 associates the security controls from NIST SP 800-53, Revision 4, Appendix F with the three security objectives. These associations are a factor in the development of Table D-1 and can be used to inform tailoring decisions.

The primary approach and assumptions for security control associations are:

- Each control and/or enhancement is allocated based on whether or not the security objective(s) are the *primary* focus of the control and/or enhancement. If a security objective is only indirectly affected by a control and/or enhancement, it is not associated with that control and/or enhancement.