NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

Note that NIST Special Publication (SP) 800-53B contains additional background, scoping, and implementation guidance in addition to the controls and baselines.

This PDF is produced from OSCAL Source data and represents a derivative format of controls defined in NIST SP 800-53B, ***Control Baselines for Information Systems and Organizations.*** This version contains only the control baseline tables.

If there are any discrepancies noted in the content between this NIST SP 800-53B derivative data format and the latest published NIST SP 800-53, Revision 5 ***(normative***) and NIST SP 800-53B ***(normative)***, please contact sec-cert@nist.gov and refer to the official published documents.

NIST SP 800-53B is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53B

National Institute of Standards and Technology
U.S. Department of Commerce

3.1 ACCESS CONTROL FAMILY

Table 3-1 provides a summary of the controls and control enhancements assigned to the Access Control Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-1: ACCESS CONTROL FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-1	**Policy and Procedures**	x	x	x	x
AC-2	**Account Management**		x	x	x
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT			x	x
AC-2(2)	AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT			x	x
AC-2(3)	DISABLE ACCOUNTS			x	x
AC-2(4)	AUTOMATED AUDIT ACTIONS			x	x
AC-2(5)	INACTIVITY LOGOUT			x	x
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT				
AC-2(7)	PRIVILEGED USER ACCOUNTS				
AC-2(8)	DYNAMIC ACCOUNT MANAGEMENT				
AC-2(9)	RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS				
AC-2(10)	SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE	W: Incorporated into AC-2.			
AC-2(11)	USAGE CONDITIONS				x
AC-2(12)	ACCOUNT MONITORING FOR ATYPICAL USAGE				x
AC-2(13)	DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS			x	x
AC-3	**Access Enforcement**		x	x	x
AC-3(1)	RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS	W: Incorporated into AC-6.			
AC-3(2)	DUAL AUTHORIZATION				
AC-3(3)	MANDATORY ACCESS CONTROL				
AC-3(4)	DISCRETIONARY ACCESS CONTROL				
AC-3(5)	SECURITY-RELEVANT INFORMATION				
AC-3(6)	PROTECTION OF USER AND SYSTEM INFORMATION	W: Incorporated into MP-4 and SC-28.			
AC-3(7)	ROLE-BASED ACCESS CONTROL				
AC-3(8)	REVOCATION OF ACCESS AUTHORIZATIONS				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-3(9)	CONTROLLED RELEASE				
AC-3(10)	AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS				
AC-3(11)	RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES				
AC-3(12)	ASSERT AND ENFORCE APPLICATION ACCESS				
AC-3(13)	ATTRIBUTE-BASED ACCESS CONTROL				
AC-3(14)	INDIVIDUAL ACCESS	x			
AC-3(15)	DISCRETIONARY AND MANDATORY ACCESS CONTROL				
AC-4	**Information Flow Enforcement**			x	x
AC-4(1)	OBJECT SECURITY AND PRIVACY ATTRIBUTES				
AC-4(2)	PROCESSING DOMAINS				
AC-4(3)	DYNAMIC INFORMATION FLOW CONTROL				
AC-4(4)	FLOW CONTROL OF ENCRYPTED INFORMATION				x
AC-4(5)	EMBEDDED DATA TYPES				
AC-4(6)	METADATA				
AC-4(7)	ONE-WAY FLOW MECHANISMS				
AC-4(8)	SECURITY AND PRIVACY POLICY FILTERS				
AC-4(9)	HUMAN REVIEWS				
AC-4(10)	ENABLE AND DISABLE SECURITY OR PRIVACY POLICY FILTERS				
AC-4(11)	CONFIGURATION OF SECURITY OR PRIVACY POLICY FILTERS				
AC-4(12)	DATA TYPE IDENTIFIERS				
AC-4(13)	DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS				
AC-4(14)	SECURITY OR PRIVACY POLICY FILTER CONSTRAINTS				
AC-4(15)	DETECTION OF UNSANCTIONED INFORMATION				
AC-4(16)	INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS	W: Incorporated into AC-4.			
AC-4(17)	DOMAIN AUTHENTICATION				
AC-4(18)	SECURITY ATTRIBUTE BINDING	W: Incorporated into AC-16.			
AC-4(19)	VALIDATION OF METADATA				
AC-4(20)	APPROVED SOLUTIONS				
AC-4(21)	PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS				
AC-4(22)	ACCESS ONLY				
AC-4(23)	MODIFY NON-RELEASABLE INFORMATION				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-4(24)	INTERNAL NORMALIZED FORMAT				
AC-4(25)	DATA SANITIZATION				
AC-4(26)	AUDIT FILTERING ACTIONS				
AC-4(27)	REDUNDANT/INDEPENDENT FILTERING MECHANISMS				
AC-4(28)	LINEAR FILTER PIPELINES				
AC-4(29)	FILTER ORCHESTRATION ENGINES				
AC-4(30)	FILTER MECHANISMS USING MULTIPLE PROCESSES				
AC-4(31)	FAILED CONTENT TRANSFER PREVENTION				
AC-4(32)	PROCESS REQUIREMENTS FOR INFORMATION TRANSFER				
AC-5	**Separation of Duties**			x	x
AC-6	**Least Privilege**			x	x
AC-6(1)	AUTHORIZE ACCESS TO SECURITY FUNCTIONS			x	x
AC-6(2)	NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS			x	x
AC-6(3)	NETWORK ACCESS TO PRIVILEGED COMMANDS				x
AC-6(4)	SEPARATE PROCESSING DOMAINS				
AC-6(5)	PRIVILEGED ACCOUNTS			x	x
AC-6(6)	PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS				
AC-6(7)	REVIEW OF USER PRIVILEGES			x	x
AC-6(8)	PRIVILEGE LEVELS FOR CODE EXECUTION				
AC-6(9)	LOG USE OF PRIVILEGED FUNCTIONS			x	x
AC-6(10)	PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS			x	x
AC-7	**Unsuccessful Logon Attempts**		x	x	x
AC-7(1)	AUTOMATIC ACCOUNT LOCK	W: Incorporated into AC-7.			
AC-7(2)	PURGE OR WIPE MOBILE DEVICE				
AC-7(3)	BIOMETRIC ATTEMPT LIMITING				
AC-7(4)	USE OF ALTERNATE AUTHENTICATION FACTOR				
AC-8	**System Use Notification**		x	x	x
AC-9	**Previous Logon Notification**				
AC-9(1)	UNSUCCESSFUL LOGONS				
AC-9(2)	SUCCESSFUL AND UNSUCCESSFUL LOGONS				
AC-9(3)	NOTIFICATION OF ACCOUNT CHANGES				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-9(4)	ADDITIONAL LOGON INFORMATION				
AC-10	**Concurrent Session Control**				x
AC-11	**Device Lock**			x	x
AC-11(1)	PATTERN-HIDING DISPLAYS			x	x
AC-12	**Session Termination**			x	x
AC-12(1)	USER-INITIATED LOGOUTS				
AC-12(2)	TERMINATION MESSAGE				
AC-12(3)	TIMEOUT WARNING MESSAGE				
AC-13	**Supervision and Review — Access Control**	W: Incorporated into AC-2 and AU-6.			
AC-14	**Permitted Actions Without Identification or Authentication**		x	x	x
AC-14(1)	NECESSARY USES	W: Incorporated into AC-14.			
AC-15	**Automated Marking**	W: Incorporated into MP-3.			
AC-16	**Security and Privacy Attributes**				
AC-16(1)	DYNAMIC ATTRIBUTE ASSOCIATION				
AC-16(2)	ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS				
AC-16(3)	MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM				
AC-16(4)	ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS				
AC-16(5)	ATTRIBUTE DISPLAYS ON OBJECTS TO BE OUTPUT				
AC-16(6)	MAINTENANCE OF ATTRIBUTE ASSOCIATION				
AC-16(7)	CONSISTENT ATTRIBUTE INTERPRETATION				
AC-16(8)	ASSOCIATION TECHNIQUES AND TECHNOLOGIES				
AC-16(9)	ATTRIBUTE REASSIGNMENT — REGRADING MECHANISMS				
AC-16(10)	ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS				
AC-17	**Remote Access**		x	x	x
AC-17(1)	MONITORING AND CONTROL			x	x
AC-17(2)	PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION			x	x
AC-17(3)	MANAGED ACCESS CONTROL POINTS			x	x
AC-17(4)	PRIVILEGED COMMANDS AND ACCESS			x	x
AC-17(5)	MONITORING FOR UNAUTHORIZED CONNECTIONS	W: Incorporated into SI-4.			
AC-17(6)	PROTECTION OF MECHANISM INFORMATION				
AC-17(7)	ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS	W: Incorporated into AC-3(10).			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-17(8)	DISABLE NONSECURE NETWORK PROTOCOLS	W: Incorporated into CM-7.			
AC-17(9)	DISCONNECT OR DISABLE ACCESS				
AC-17(10)	AUTHENTICATE REMOTE COMMANDS				
AC-18	**Wireless Access**		x	x	x
AC-18(1)	AUTHENTICATION AND ENCRYPTION			x	x
AC-18(2)	MONITORING UNAUTHORIZED CONNECTIONS	W: Incorporated into SI-4.			
AC-18(3)	DISABLE WIRELESS NETWORKING			x	x
AC-18(4)	RESTRICT CONFIGURATIONS BY USERS				x
AC-18(5)	ANTENNAS AND TRANSMISSION POWER LEVELS				x
AC-19	**Access Control for Mobile Devices**		x	x	x
AC-19(1)	USE OF WRITABLE AND PORTABLE STORAGE DEVICES	W: Incorporated into MP-7.			
AC-19(2)	USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES	W: Incorporated into MP-7.			
AC-19(3)	USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER	W: Incorporated into MP-7.			
AC-19(4)	RESTRICTIONS FOR CLASSIFIED INFORMATION				
AC-19(5)	FULL DEVICE OR CONTAINER-BASED ENCRYPTION			x	x
AC-20	**Use of External Systems**		x	x	x
AC-20(1)	LIMITS ON AUTHORIZED USE			x	x
AC-20(2)	PORTABLE STORAGE DEVICES — RESTRICTED USE			x	x
AC-20(3)	NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE				
AC-20(4)	NETWORK ACCESSIBLE STORAGE DEVICES — PROHIBITED USE				
AC-20(5)	PORTABLE STORAGE DEVICES — PROHIBITED USE				
AC-21	**Information Sharing**			x	x
AC-21(1)	AUTOMATED DECISION SUPPORT				
AC-21(2)	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)	TRANSMIT ACCESS AUTHORIZATION INFORMATION				
AC-24(2)	NO USER OR PROCESS IDENTITY				
AC-25	**Reference Monitor**				

3.2 AWARENESS AND TRAINING FAMILY

Table 3-2 provides a summary of the controls and control enhancements assigned to the Awareness and Training Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-2: AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	**Policy and Procedures**	x	x	x	x
AT-2	**Literacy Training and Awareness**	x	x	x	x
AT-2(1)	PRACTICAL EXERCISES				
AT-2(2)	INSIDER THREAT		x	x	x
AT-2(3)	SOCIAL ENGINEERING AND MINING			x	x
AT-2(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR				
AT-2(5)	ADVANCED PERSISTENT THREAT				
AT-2(6)	CYBER THREAT ENVIRONMENT				
AT-3	**Role-based Training**	x	x	x	x
AT-3(1)	ENVIRONMENTAL CONTROLS				
AT-3(2)	PHYSICAL SECURITY CONTROLS				
AT-3(3)	PRACTICAL EXERCISES				
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	W: Incorporated into AT-2(4).			
AT-3(5)	PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	x			
AT-4	**Training Records**	x	x	x	x
AT-5	**Contacts with Security Groups and Associations**	W: Incorporated into PM-15.			
AT-6	**Training Feedback**				

3.3 AUDIT AND ACCOUNTABILITY FAMILY

Table 3-3 provides a summary of the controls and control enhancements assigned to the Audit and Accountability Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-3: AUDIT AND ACCOUNTABILITY FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AU-1	**Policy and Procedures**	x	x	x	x
AU-2	**Event Logging**	x	x	x	x
AU-2(1)	COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES	W: Incorporated into AU-12.			
AU-2(2)	SELECTION OF AUDIT EVENTS BY COMPONENT	W: Incorporated into AU-12.			
AU-2(3)	REVIEWS AND UPDATES	W: Incorporated into AU-2.			
AU-2(4)	PRIVILEGED FUNCTIONS	W: Incorporated into AC-6(9).			
AU-3	**Content of Audit Records**		x	x	x
AU-3(1)	ADDITIONAL AUDIT INFORMATION			x	x
AU-3(2)	CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT	W: Incorporated into PL-9.			
AU-3(3)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	x			
AU-4	**Audit Log Storage Capacity**		x	x	x
AU-4(1)	TRANSFER TO ALTERNATE STORAGE				
AU-5	**Response to Audit Logging Process Failures**		x	x	x
AU-5(1)	STORAGE CAPACITY WARNING				x
AU-5(2)	REAL-TIME ALERTS				x
AU-5(3)	CONFIGURABLE TRAFFIC VOLUME THRESHOLDS				
AU-5(4)	SHUTDOWN ON FAILURE				
AU-5(5)	ALTERNATE AUDIT LOGGING CAPABILITY				
AU-6	**Audit Record Review, Analysis, and Reporting**		x	x	x
AU-6(1)	AUTOMATED PROCESS INTEGRATION			x	x
AU-6(2)	AUTOMATED SECURITY ALERTS	W: Incorporated into SI-4.			
AU-6(3)	CORRELATE AUDIT RECORD REPOSITORIES			x	x
AU-6(4)	CENTRAL REVIEW AND ANALYSIS				
AU-6(5)	INTEGRATED ANALYSIS OF AUDIT RECORDS				x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AU-6(6)	CORRELATION WITH PHYSICAL MONITORING				x
AU-6(7)	PERMITTED ACTIONS				
AU-6(8)	FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS				
AU-6(9)	CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES				
AU-6(10)	AUDIT LEVEL ADJUSTMENT	W: Incorporated into AU-6.			
AU-7	**Audit Record Reduction and Report Generation**			x	x
AU-7(1)	AUTOMATIC PROCESSING			x	x
AU-7(2)	AUTOMATIC SORT AND SEARCH	W: Incorporated into AU-7(1).			
AU-8	**Time Stamps**		x	x	x
AU-8(1)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	W: Moved to SC-45(1).			
AU-8(2)	SECONDARY AUTHORITATIVE TIME SOURCE	W: Moved to SC-45(2).			
AU-9	**Protection of Audit Information**		x	x	x
AU-9(1)	HARDWARE WRITE-ONCE MEDIA				
AU-9(2)	STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS				x
AU-9(3)	CRYPTOGRAPHIC PROTECTION				x
AU-9(4)	ACCESS BY SUBSET OF PRIVILEGED USERS			x	x
AU-9(5)	DUAL AUTHORIZATION				
AU-9(6)	READ-ONLY ACCESS				
AU-9(7)	STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM				
AU-10	**Non-repudiation**				x
AU-10(1)	ASSOCIATION OF IDENTITIES				
AU-10(2)	VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY				
AU-10(3)	CHAIN OF CUSTODY				
AU-10(4)	VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY				
AU-10(5)	DIGITAL SIGNATURES	W: Incorporated into SI-7.			
AU-11	**Audit Record Retention**	x	x	x	x
AU-11(1)	LONG-TERM RETRIEVAL CAPABILITY				
AU-12	**Audit Record Generation**		x	x	x
AU-12(1)	SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL				x
AU-12(2)	STANDARDIZED FORMATS				
AU-12(3)	CHANGES BY AUTHORIZED INDIVIDUALS				x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AU-12(4)	QUERY PARAMETER AUDITS OF PERSONALLY IDENTIFIABLE INFORMATION				
AU-13	**Monitoring for Information Disclosure**				
AU-13(1)	USE OF AUTOMATED TOOLS				
AU-13(2)	REVIEW OF MONITORED SITES				
AU-13(3)	UNAUTHORIZED REPLICATION OF INFORMATION				
AU-14	**Session Audit**				
AU-14(1)	SYSTEM START-UP				
AU-14(2)	CAPTURE AND RECORD CONTENT	W: Incorporated into AU-14.			
AU-14(3)	REMOTE VIEWING AND LISTENING				
AU-15	**Alternate Audit Logging Capability**	W: Moved to AU-5(5).			
AU-16	**Cross-organizational Audit Logging**				
AU-16(1)	IDENTITY PRESERVATION				
AU-16(2)	SHARING OF AUDIT INFORMATION				
AU-16(3)	DISASSOCIABILITY				

3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING FAMILY

Table 3-4 provides a summary of the controls and control enhancements assigned to the Assessment, Authorization, and Monitoring Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-4: ASSESSMENT, AUTHORIZATION, AND MONITORING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CA-1	**Policy and Procedures**	x	x	x	x
CA-2	**Control Assessments**	x	x	x	x
CA-2(1)	INDEPENDENT ASSESSORS			x	x
CA-2(2)	SPECIALIZED ASSESSMENTS				x
CA-2(3)	LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS				
CA-3	**Information Exchange**		x	x	x
CA-3(1)	UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(25).			
CA-3(2)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(26).			
CA-3(3)	UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(27).			
CA-3(4)	CONNECTIONS TO PUBLIC NETWORKS	W: Moved to SC-7(28).			
CA-3(5)	RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS	W: Incorporated into SC-7(5).			
CA-3(6)	TRANSFER AUTHORIZATIONS				x
CA-3(7)	TRANSITIVE INFORMATION EXCHANGES				
CA-4	**Security Certification**	W: Incorporated into CA-2.			
CA-5	**Plan of Action and Milestones**	x	x	x	x
CA-5(1)	AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY				
CA-6	**Authorization**	x	x	x	x
CA-6(1)	JOINT AUTHORIZATION — INTRA-ORGANIZATION				
CA-6(2)	JOINT AUTHORIZATION — INTER-ORGANIZATION				
CA-7	**Continuous Monitoring**	x	x	x	x
CA-7(1)	INDEPENDENT ASSESSMENT			x	x
CA-7(2)	TYPES OF ASSESSMENTS	W: Incorporated into CA-2.			
CA-7(3)	TREND ANALYSES				
CA-7(4)	RISK MONITORING	x	x	x	x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CA-7(5)	CONSISTENCY ANALYSIS				
CA-7(6)	AUTOMATION SUPPORT FOR MONITORING				
CA-8	**Penetration Testing**				x
CA-8(1)	INDEPENDENT PENETRATION TESTING AGENT OR TEAM				x
CA-8(2)	RED TEAM EXERCISES				
CA-8(3)	FACILITY PENETRATION TESTING				
CA-9	**Internal System Connections**		x	x	x
CA-9(1)	COMPLIANCE CHECKS				

3.5 CONFIGURATION MANAGEMENT FAMILY

Table 3-5 provides a summary of the controls and control enhancements assigned to the Configuration Management Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-5: CONFIGURATION MANAGEMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CM-1	**Policy and Procedures**	x	x	x	x
CM-2	**Baseline Configuration**		x	x	x
CM-2(1)	REVIEWS AND UPDATES	W: Incorporated into CM-2.			
CM-2(2)	AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY			x	x
CM-2(3)	RETENTION OF PREVIOUS CONFIGURATIONS			x	x
CM-2(4)	UNAUTHORIZED SOFTWARE	W: Incorporated into CM-7(4).			
CM-2(5)	AUTHORIZED SOFTWARE	W: Incorporated into CM-7(5).			
CM-2(6)	DEVELOPMENT AND TEST ENVIRONMENTS				
CM-2(7)	CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS			x	x
CM-3	**Configuration Change Control**			x	x
CM-3(1)	AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES				x
CM-3(2)	TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES			x	x
CM-3(3)	AUTOMATED CHANGE IMPLEMENTATION				
CM-3(4)	SECURITY AND PRIVACY REPRESENTATIVES			x	x
CM-3(5)	AUTOMATED SECURITY RESPONSE				
CM-3(6)	CRYPTOGRAPHY MANAGEMENT				x
CM-3(7)	REVIEW SYSTEM CHANGES				
CM-3(8)	PREVENT OR RESTRICT CONFIGURATION CHANGES				
CM-4	**Impact Analyses**	x	x	x	x
CM-4(1)	SEPARATE TEST ENVIRONMENTS				x
CM-4(2)	VERIFICATION OF CONTROLS			x	x
CM-5	**Access Restrictions for Change**		x	x	x
CM-5(1)	AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS				x
CM-5(2)	REVIEW SYSTEM CHANGES	W: Incorporated into CM-3(7).			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CM-5(3)	SIGNED COMPONENTS	W: Moved to CM-14.			
CM-5(4)	DUAL AUTHORIZATION				
CM-5(5)	PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION				
CM-5(6)	LIMIT LIBRARY PRIVILEGES				
CM-5(7)	AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS	W: Incorporated into SI-7.			
CM-6	**Configuration Settings**		x	x	x
CM-6(1)	AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION				x
CM-6(2)	RESPOND TO UNAUTHORIZED CHANGES				x
CM-6(3)	UNAUTHORIZED CHANGE DETECTION	W: Incorporated into SI-7.			
CM-6(4)	CONFORMANCE DEMONSTRATION	W: Incorporated into CM-4.			
CM-7	**Least Functionality**		x	x	x
CM-7(1)	PERIODIC REVIEW			x	x
CM-7(2)	PREVENT PROGRAM EXECUTION			x	x
CM-7(3)	REGISTRATION COMPLIANCE				
CM-7(4)	UNAUTHORIZED SOFTWARE — DENY-BY-EXCEPTION				
CM-7(5)	AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION			x	x
CM-7(6)	CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES				
CM-7(7)	CODE EXECUTION IN PROTECTED ENVIRONMENTS				
CM-7(8)	BINARY OR MACHINE EXECUTABLE CODE				
CM-7(9)	PROHIBITING THE USE OF UNAUTHORIZED HARDWARE				
CM-8	**System Component Inventory**		x	x	x
CM-8(1)	UPDATES DURING INSTALLATION AND REMOVAL			x	x
CM-8(2)	AUTOMATED MAINTENANCE				x
CM-8(3)	AUTOMATED UNAUTHORIZED COMPONENT DETECTION			x	x
CM-8(4)	ACCOUNTABILITY INFORMATION				x
CM-8(5)	NO DUPLICATE ACCOUNTING OF COMPONENTS	W: Incorporated into CM-8.			
CM-8(6)	ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS				
CM-8(7)	CENTRALIZED REPOSITORY				
CM-8(8)	AUTOMATED LOCATION TRACKING				
CM-8(9)	ASSIGNMENT OF COMPONENTS TO SYSTEMS				
CM-9	**Configuration Management Plan**			x	x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CM-9(1)	ASSIGNMENT OF RESPONSIBILITY				
CM-10	**Software Usage Restrictions**		x	x	x
CM-10(1)	OPEN-SOURCE SOFTWARE				
CM-11	**User-installed Software**		x	x	x
CM-11(1)	ALERTS FOR UNAUTHORIZED INSTALLATIONS	W: Incorporated into CM-8(3).			
CM-11(2)	SOFTWARE INSTALLATION WITH PRIVILEGED STATUS				
CM-11(3)	AUTOMATED ENFORCEMENT AND MONITORING				
CM-12	**Information Location**			x	x
CM-12(1)	AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION			x	x
CM-13	**Data Action Mapping**				
CM-14	**Signed Components**				

3.6 CONTINGENCY PLANNING FAMILY

Table 3-6 provides a summary of the controls and control enhancements assigned to the Contingency Planning Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-6: CONTINGENCY PLANNING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CP-1	**Policy and Procedures**		x	x	x
CP-2	**Contingency Plan**		x	x	x
CP-2(1)	COORDINATE WITH RELATED PLANS			x	x
CP-2(2)	CAPACITY PLANNING				x
CP-2(3)	RESUME MISSION AND BUSINESS FUNCTIONS			x	x
CP-2(4)	RESUME ALL MISSION AND BUSINESS FUNCTIONS	W: Incorporated into CP-2(3).			
CP-2(5)	CONTINUE MISSION AND BUSINESS FUNCTIONS				x
CP-2(6)	ALTERNATE PROCESSING AND STORAGE SITES				
CP-2(7)	COORDINATE WITH EXTERNAL SERVICE PROVIDERS				
CP-2(8)	IDENTIFY CRITICAL ASSETS			x	x
CP-3	**Contingency Training**		x	x	x
CP-3(1)	SIMULATED EVENTS				x
CP-3(2)	MECHANISMS USED IN TRAINING ENVIRONMENTS				
CP-4	**Contingency Plan Testing**		x	x	x
CP-4(1)	COORDINATE WITH RELATED PLANS			x	x
CP-4(2)	ALTERNATE PROCESSING SITE				x
CP-4(3)	AUTOMATED TESTING				
CP-4(4)	FULL RECOVERY AND RECONSTITUTION				
CP-4(5)	SELF-CHALLENGE				
CP-5	**Contingency Plan Update**	W: Incorporated into CP-2.			
CP-6	**Alternate Storage Site**			x	x
CP-6(1)	SEPARATION FROM PRIMARY SITE			x	x
CP-6(2)	RECOVERY TIME AND RECOVERY POINT OBJECTIVES				x
CP-6(3)	ACCESSIBILITY			x	x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CP-7	**Alternate Processing Site**			x	x
CP-7(1)	SEPARATION FROM PRIMARY SITE			x	x
CP-7(2)	ACCESSIBILITY			x	x
CP-7(3)	PRIORITY OF SERVICE			x	x
CP-7(4)	PREPARATION FOR USE				x
CP-7(5)	EQUIVALENT INFORMATION SECURITY SAFEGUARDS	W: Incorporated into CP-7.			
CP-7(6)	INABILITY TO RETURN TO PRIMARY SITE				
CP-8	**Telecommunications Services**			x	x
CP-8(1)	PRIORITY OF SERVICE PROVISIONS			x	x
CP-8(2)	SINGLE POINTS OF FAILURE			x	x
CP-8(3)	SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS				x
CP-8(4)	PROVIDER CONTINGENCY PLAN				x
CP-8(5)	ALTERNATE TELECOMMUNICATION SERVICE TESTING				
CP-9	**System Backup**		x	x	x
CP-9(1)	TESTING FOR RELIABILITY AND INTEGRITY			x	x
CP-9(2)	TEST RESTORATION USING SAMPLING				x
CP-9(3)	SEPARATE STORAGE FOR CRITICAL INFORMATION				x
CP-9(4)	PROTECTION FROM UNAUTHORIZED MODIFICATION	W: Incorporated into CP-9.			
CP-9(5)	TRANSFER TO ALTERNATE STORAGE SITE				x
CP-9(6)	REDUNDANT SECONDARY SYSTEM				
CP-9(7)	DUAL AUTHORIZATION FOR DELETION OR DESTRUCTION				
CP-9(8)	CRYPTOGRAPHIC PROTECTION			x	x
CP-10	**System Recovery and Reconstitution**		x	x	x
CP-10(1)	CONTINGENCY PLAN TESTING	W: Incorporated into CP-4.			
CP-10(2)	TRANSACTION RECOVERY			x	x
CP-10(3)	COMPENSATING SECURITY CONTROLS	W: Addressed through tailoring.			
CP-10(4)	RESTORE WITHIN TIME PERIOD				x
CP-10(5)	FAILOVER CAPABILITY	W: Incorporated into SI-13.			
CP-10(6)	COMPONENT PROTECTION				
CP-11	**Alternate Communications Protocols**				
CP-12	**Safe Mode**				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CP-13	**Alternative Security Mechanisms**				

3.7 IDENTIFICATION AND AUTHENTICATION FAMILY

Table 3-7 provides a summary of the controls and control enhancements assigned to the Identification and Authentication Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-7: IDENTIFICATION AND AUTHENTICATION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IA-1	**Policy and Procedures**		x	x	x
IA-2	**Identification and Authentication (Organizational Users)**		x	x	x
IA-2(1)	MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS		x	x	x
IA-2(2)	MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS		x	x	x
IA-2(3)	LOCAL ACCESS TO PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(1).			
IA-2(4)	LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(2).			
IA-2(5)	INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION				x
IA-2(6)	ACCESS TO ACCOUNTS —SEPARATE DEVICE				
IA-2(7)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — SEPARATE DEVICE	W: Incorporated into IA-2(6).			
IA-2(8)	ACCESS TO ACCOUNTS — REPLAY RESISTANT		x	x	x
IA-2(9)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — REPLAY RESISTANT	W: Incorporated into IA-2(8).			
IA-2(10)	SINGLE SIGN-ON				
IA-2(11)	REMOTE ACCESS — SEPARATE DEVICE	W: Incorporated into IA-2(6).			
IA-2(12)	ACCEPTANCE OF PIV CREDENTIALS		x	x	x
IA-2(13)	OUT-OF-BAND AUTHENTICATION				
IA-3	**Device Identification and Authentication**			x	x
IA-3(1)	CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION				
IA-3(2)	CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION	W: Incorporated into IA-3(1).			
IA-3(3)	DYNAMIC ADDRESS ALLOCATION				
IA-3(4)	DEVICE ATTESTATION				
IA-4	**Identifier Management**		x	x	x
IA-4(1)	PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS				
IA-4(2)	SUPERVISOR AUTHORIZATION	W: Incorporated into IA-12(1).			
IA-4(3)	MULTIPLE FORMS OF CERTIFICATION	W: Incorporated into IA-12(2).			
IA-4(4)	IDENTIFY USER STATUS			x	x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IA-4(5)	DYNAMIC MANAGEMENT				
IA-4(6)	CROSS-ORGANIZATION MANAGEMENT				
IA-4(7)	IN-PERSON REGISTRATION	W: Incorporated into IA-12(4).			
IA-4(8)	PAIRWISE PSEUDONYMOUS IDENTIFIERS				
IA-4(9)	ATTRIBUTE MAINTENANCE AND PROTECTION				
IA-5	**Authenticator Management**		x	x	x
IA-5(1)	PASSWORD-BASED AUTHENTICATION		x	x	x
IA-5(2)	PUBLIC KEY-BASED AUTHENTICATION			x	x
IA-5(3)	IN-PERSON OR TRUSTED EXTERNAL PARTY REGISTRATION	W: Incorporated into IA-12(4).			
IA-5(4)	AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION	W: Incorporated into IA-5(1).			
IA-5(5)	CHANGE AUTHENTICATORS PRIOR TO DELIVERY				
IA-5(6)	PROTECTION OF AUTHENTICATORS			x	x
IA-5(7)	NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS				
IA-5(8)	MULTIPLE SYSTEM ACCOUNTS				
IA-5(9)	FEDERATED CREDENTIAL MANAGEMENT				
IA-5(10)	DYNAMIC CREDENTIAL BINDING				
IA-5(11)	HARDWARE TOKEN-BASED AUTHENTICATION	W: Incorporated into IA-2(1) and IA-2(2).			
IA-5(12)	BIOMETRIC AUTHENTICATION PERFORMANCE				
IA-5(13)	EXPIRATION OF CACHED AUTHENTICATORS				
IA-5(14)	MANAGING CONTENT OF PKI TRUST STORES				
IA-5(15)	GSA-APPROVED PRODUCTS AND SERVICES				
IA-5(16)	IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE				
IA-5(17)	PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS				
IA-5(18)	PASSWORD MANAGERS				
IA-6	**Authentication 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)	ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES		x	x	x
IA-8(2)	ACCEPTANCE OF EXTERNAL AUTHENTICATORS		x	x	x
IA-8(3)	USE OF FICAM-APPROVED PRODUCTS	W: Incorporated into IA-8(2).			
IA-8(4)	USE OF DEFINED PROFILES		x	x	x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IA-8(5)	ACCEPTANCE OF PIV-I CREDENTIALS				
IA-8(6)	DISASSOCIABILITY				
IA-9	**Service Identification and Authentication**				
IA-9(1)	INFORMATION EXCHANGE	W: Incorporated into IA-9.			
IA-9(2)	TRANSMISSION OF DECISIONS	W: Incorporated into IA-9.			
IA-10	**Adaptive Authentication**				
IA-11	**Re-authentication**		x	x	x
IA-12	**Identity Proofing**			x	x
IA-12(1)	SUPERVISOR AUTHORIZATION				
IA-12(2)	IDENTITY EVIDENCE			x	x
IA-12(3)	IDENTITY EVIDENCE VALIDATION AND VERIFICATION			x	x
IA-12(4)	IN-PERSON VALIDATION AND VERIFICATION				x
IA-12(5)	ADDRESS CONFIRMATION			x	x
IA-12(6)	ACCEPT EXTERNALLY-PROOFED IDENTITIES				

3.8 INCIDENT RESPONSE FAMILY

Table 3-8 provides a summary of the controls and control enhancements assigned to the Incident Response Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-8: INCIDENT RESPONSE FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IR-1	**Policy and Procedures**	x	x	x	x
IR-2	**Incident Response Training**	x	x	x	x
IR-2(1)	SIMULATED EVENTS				x
IR-2(2)	AUTOMATED TRAINING ENVIRONMENTS				x
IR-2(3)	BREACH	x			
IR-3	**Incident Response Testing**	x		x	x
IR-3(1)	AUTOMATED TESTING				
IR-3(2)	COORDINATION WITH RELATED PLANS			x	x
IR-3(3)	CONTINUOUS IMPROVEMENT				
IR-4	**Incident Handling**	x	x	x	x
IR-4(1)	AUTOMATED INCIDENT HANDLING PROCESSES			x	x
IR-4(2)	DYNAMIC RECONFIGURATION				
IR-4(3)	CONTINUITY OF OPERATIONS				
IR-4(4)	INFORMATION CORRELATION				x
IR-4(5)	AUTOMATIC DISABLING OF SYSTEM				
IR-4(6)	INSIDER THREATS				
IR-4(7)	INSIDER THREATS — INTRA-ORGANIZATION COORDINATION				
IR-4(8)	CORRELATION WITH EXTERNAL ORGANIZATIONS				
IR-4(9)	DYNAMIC RESPONSE CAPABILITY				
IR-4(10)	SUPPLY CHAIN COORDINATION				
IR-4(11)	INTEGRATED INCIDENT RESPONSE TEAM				x
IR-4(12)	MALICIOUS CODE AND FORENSIC ANALYSIS				
IR-4(13)	BEHAVIOR ANALYSIS				
IR-4(14)	SECURITY OPERATIONS CENTER				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IR-4(15)	PUBLIC RELATIONS AND REPUTATION REPAIR				
IR-5	**Incident Monitoring**	x	x	x	x
IR-5(1)	AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS				x
IR-6	**Incident Reporting**	x	x	x	x
IR-6(1)	AUTOMATED REPORTING			x	x
IR-6(2)	VULNERABILITIES RELATED TO INCIDENTS				
IR-6(3)	SUPPLY CHAIN COORDINATION			x	x
IR-7	**Incident Response Assistance**	x	x	x	x
IR-7(1)	AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT			x	x
IR-7(2)	COORDINATION WITH EXTERNAL PROVIDERS				
IR-8	**Incident Response Plan**	x	x	x	x
IR-8(1)	BREACHES	x			
IR-9	**Information Spillage Response**				
IR-9(1)	RESPONSIBLE PERSONNEL	W: Incorporated into IR-9.			
IR-9(2)	TRAINING				
IR-9(3)	POST-SPILL OPERATIONS				
IR-9(4)	EXPOSURE TO UNAUTHORIZED PERSONNEL				
IR-10	**Integrated Information Security Analysis Team**	W: Moved to IR-4(11).			

3.9 MAINTENANCE FAMILY

Table 3-9 provides a summary of the controls and control enhancements assigned to the Maintenance Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-9: MAINTENANCE FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
MA-1	**Policy and Procedures**		x	x	x
MA-2	**Controlled Maintenance**		x	x	x
MA-2(1)	RECORD CONTENT	W: Incorporated into MA-2.			
MA-2(2)	AUTOMATED MAINTENANCE ACTIVITIES				x
MA-3	**Maintenance Tools**			x	x
MA-3(1)	INSPECT TOOLS			x	x
MA-3(2)	INSPECT MEDIA			x	x
MA-3(3)	PREVENT UNAUTHORIZED REMOVAL			x	x
MA-3(4)	RESTRICTED TOOL USE				
MA-3(5)	EXECUTION WITH PRIVILEGE				
MA-3(6)	SOFTWARE UPDATES AND PATCHES				
MA-4	**Nonlocal Maintenance**		x	x	x
MA-4(1)	LOGGING AND REVIEW				
MA-4(2)	DOCUMENT NONLOCAL MAINTENANCE	W: Incorporated into MA-1 and MA-4.			
MA-4(3)	COMPARABLE SECURITY AND SANITIZATION				x
MA-4(4)	AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS				
MA-4(5)	APPROVALS AND NOTIFICATIONS				
MA-4(6)	CRYPTOGRAPHIC PROTECTION				
MA-4(7)	DISCONNECT VERIFICATION				
MA-5	**Maintenance Personnel**		x	x	x
MA-5(1)	INDIVIDUALS WITHOUT APPROPRIATE ACCESS				x
MA-5(2)	SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS				
MA-5(3)	CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
MA-5(4)	FOREIGN NATIONALS				
MA-5(5)	NON-SYSTEM MAINTENANCE				
MA-6	**Timely Maintenance**			x	x
MA-6(1)	PREVENTIVE MAINTENANCE				
MA-6(2)	PREDICTIVE MAINTENANCE				
MA-6(3)	AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE				
MA-7	**Field Maintenance**				

3.10 MEDIA PROTECTION FAMILY

Table 3-10 provides a summary of the controls and control enhancements assigned to the Media Protection Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-10: MEDIA PROTECTION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
MP-1	**Policy and Procedures**	x	x	x	x
MP-2	**Media Access**		x	x	x
MP-2(1)	AUTOMATED RESTRICTED ACCESS	W: Incorporated into MP-4(2).			
MP-2(2)	CRYPTOGRAPHIC PROTECTION	W: Incorporated into SC-28(1).			
MP-3	**Media Marking**			x	x
MP-4	**Media Storage**			x	x
MP-4(1)	CRYPTOGRAPHIC PROTECTION	W: Incorporated into SC-28(1).			
MP-4(2)	AUTOMATED RESTRICTED ACCESS				
MP-5	**Media Transport**			x	x
MP-5(1)	PROTECTION OUTSIDE OF CONTROLLED AREAS	W: Incorporated into MP-5.			
MP-5(2)	DOCUMENTATION OF ACTIVITIES	W: Incorporated into MP-5.			
MP-5(3)	CUSTODIANS				
MP-5(4)	CRYPTOGRAPHIC PROTECTION	W: Incorporated into SC-28(1).			
MP-6	**Media Sanitization**	x	x	x	x
MP-6(1)	REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY				x
MP-6(2)	EQUIPMENT TESTING				x
MP-6(3)	NONDESTRUCTIVE TECHNIQUES				x
MP-6(4)	CONTROLLED UNCLASSIFIED INFORMATION	W: Incorporated into MP-6.			
MP-6(5)	CLASSIFIED INFORMATION	W: Incorporated into MP-6.			
MP-6(6)	MEDIA DESTRUCTION	W: Incorporated into MP-6.			
MP-6(7)	DUAL AUTHORIZATION				
MP-6(8)	REMOTE PURGING OR WIPING OF INFORMATION				
MP-7	**Media Use**		x	x	x
MP-7(1)	PROHIBIT USE WITHOUT OWNER	W: Incorporated into MP-7.			
MP-7(2)	PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
MP-8	**Media Downgrading**				
MP-8(1)	DOCUMENTATION OF PROCESS				
MP-8(2)	EQUIPMENT TESTING				
MP-8(3)	CONTROLLED UNCLASSIFIED INFORMATION				
MP-8(4)	CLASSIFIED INFORMATION				

3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY

Table 3-11 provides a summary of the controls and control enhancements assigned to the Physical and Environmental Protection Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-11: PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PE-1	**Policy and Procedures**		x	x	x
PE-2	**Physical Access Authorizations**		x	x	x
PE-2(1)	ACCESS BY POSITION OR ROLE				
PE-2(2)	TWO FORMS OF IDENTIFICATION				
PE-2(3)	RESTRICT UNESCORTED ACCESS				
PE-3	**Physical Access Control**		x	x	x
PE-3(1)	SYSTEM ACCESS				x
PE-3(2)	FACILITY AND SYSTEMS				
PE-3(3)	CONTINUOUS GUARDS				
PE-3(4)	LOCKABLE CASINGS				
PE-3(5)	TAMPER PROTECTION				
PE-3(6)	FACILITY PENETRATION TESTING	W: Incorporated into CA-8.			
PE-3(7)	PHYSICAL BARRIERS				
PE-3(8)	ACCESS CONTROL VESTIBULES				
PE-4	**Access Control for Transmission**			x	x
PE-5	**Access Control for Output Devices**			x	x
PE-5(1)	ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS	W: Incorporated into PE-5.			
PE-5(2)	LINK TO INDIVIDUAL IDENTITY				
PE-5(3)	MARKING OUTPUT DEVICES	W: Incorporated into PE-22.			
PE-6	**Monitoring Physical Access**		x	x	x
PE-6(1)	INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT			x	x
PE-6(2)	AUTOMATED INTRUSION RECOGNITION AND RESPONSES				
PE-6(3)	VIDEO SURVEILLANCE				
PE-6(4)	MONITORING PHYSICAL ACCESS TO SYSTEMS				x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PE-7	**Visitor Control**	W: Incorporated into PE-2 and PE-3.			
PE-8	**Visitor Access Records**		x	x	x
PE-8(1)	AUTOMATED RECORDS MAINTENANCE AND REVIEW				x
PE-8(2)	PHYSICAL ACCESS RECORDS	W: Incorporated into PE-2.			
PE-8(3)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	x			
PE-9	**Power Equipment and Cabling**			x	x
PE-9(1)	REDUNDANT CABLING				
PE-9(2)	AUTOMATIC VOLTAGE CONTROLS				
PE-10	**Emergency Shutoff**			x	x
PE-10(1)	ACCIDENTAL AND UNAUTHORIZED ACTIVATION	W: Incorporated into PE-10.			
PE-11	**Emergency Power**			x	x
PE-11(1)	ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY				x
PE-11(2)	ALTERNATE POWER SUPPLY — SELF-CONTAINED				
PE-12	**Emergency Lighting**		x	x	x
PE-12(1)	ESSENTIAL MISSION AND BUSINESS FUNCTIONS				
PE-13	**Fire Protection**		x	x	x
PE-13(1)	DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION			x	x
PE-13(2)	SUPPRESSION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION				x
PE-13(3)	AUTOMATIC FIRE SUPPRESSION	W: Incorporated into PE-13(2).			
PE-13(4)	INSPECTIONS				
PE-14	**Environmental Controls**		x	x	x
PE-14(1)	AUTOMATIC CONTROLS				
PE-14(2)	MONITORING WITH ALARMS AND NOTIFICATIONS				
PE-15	**Water Damage Protection**		x	x	x
PE-15(1)	AUTOMATION SUPPORT				x
PE-16	**Delivery and Removal**		x	x	x
PE-17	**Alternate Work Site**			x	x
PE-18	**Location of System Components**				x
PE-18(1)	FACILITY SITE	W: Moved to PE-23.			
PE-19	**Information Leakage**				
PE-19(1)	NATIONAL EMISSIONS POLICIES AND PROCEDURES				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PE-20	**Asset Monitoring and Tracking**				
PE-21	**Electromagnetic Pulse Protection**				
PE-22	**Component Marking**				
PE-23	**Facility Location**				

3.12 PLANNING FAMILY

Table 3-12 provides a summary of the controls and control enhancements assigned to the Planning Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-12: PLANNING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-1	**Policy and Procedures**	x	x	x	x
PL-2	**System Security and Privacy Plans**	x	x	x	x
PL-2(1)	CONCEPT OF OPERATIONS	W: Incorporated into PL-7.			
PL-2(2)	FUNCTIONAL ARCHITECTURE	W: Incorporated into PL-8.			
PL-2(3)	PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	W: Incorporated into PL-2.			
PL-3	**System Security Plan Update**	W: Incorporated into PL-2.			
PL-4	**Rules of Behavior**	x	x	x	x
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	x	x	x	x
PL-5	**Privacy Impact Assessment**	W: Incorporated into RA-8.			
PL-6	**Security-related Activity Planning**	W: Incorporated into PL-2.			
PL-7	**Concept of Operations**				
PL-8	**Security and Privacy Architectures**	x		x	x
PL-8(1)	DEFENSE IN DEPTH				
PL-8(2)	SUPPLIER DIVERSITY				
PL-9	**Central Management**	x			
PL-10	**Baseline Selection**		x	x	x
PL-11	**Baseline Tailoring**		x	x	x

3.13 PROGRAM MANAGEMENT FAMILY

Table 3-13 provides a summary of the controls and control enhancements assigned to the Program Management Family. These controls are implemented at the organization level and are not directed at individual information systems. The Program Management controls are designed to facilitate compliance with applicable federal laws, executive orders, directives, regulations, policies, and standards.

TABLE 3-13: PROGRAM MANAGEMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PM-1	**Information Security Program Plan**		**Deployed organization-wide.** **Supports information security program.** **Not associated with security control baselines.** **Independent of any system impact level.**		
PM-2	**Information Security Program Leadership Role**				
PM-3	**Information Security and Privacy Resources**	x			
PM-4	**Plan of Action and Milestones Process**	x			
PM-5	**System Inventory**				
PM-5(1)	INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION	x			
PM-6	**Measures of Performance**	x			
PM-7	**Enterprise Architecture**	x			
PM-7(1)	OFFLOADING				
PM-8	**Critical Infrastructure Plan**	x			
PM-9	**Risk Management Strategy**	x			
PM-10	**Authorization Process**	x			
PM-11	**Mission and Business Process Definition**	x			
PM-12	**Insider Threat Program**				
PM-13	**Security and Privacy Workforce**	x			
PM-14	**Testing, Training, and Monitoring**	x			
PM-15	**Security and Privacy Groups and Associations**				
PM-16	**Threat Awareness Program**				
PM-16(1)	AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE				
PM-17	**Protecting Controlled Unclassified Information on External Systems**	x			
PM-18	**Privacy Program Plan**	x			
PM-19	**Privacy Program Leadership Role**	x			
PM-20	**Dissemination of Privacy Program Information**	x			
PM-20(1)	PRIVACY POLICIES ON WEBSITES, APPLICATIONS, AND DIGITAL SERVICES	x			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PM-21	**Accounting of Disclosures**	x			
PM-22	**Personally Identifiable Information Quality Management**	x			
PM-23	**Data Governance Body**				
PM-24	**Data Integrity Board**	x			
PM-25	**Minimization of Personally Identifiable Information Used in Testing, Training, and Research**	x			
PM-26	**Complaint Management**	x			
PM-27	**Privacy Reporting**	x			
PM-28	**Risk Framing**	x			
PM-29	**Risk Management Program Leadership Roles**				
PM-30	**Supply Chain Risk Management Strategy**				
PM-30(1)	SUPPLIERS OF CRITICAL OR MISSION-ESSENTIAL ITEMS				
PM-31	**Continuous Monitoring Strategy**	x			
PM-32	**Purposing**				

3.14 PERSONNEL SECURITY FAMILY

Table 3-14 provides a summary of the controls and control enhancements assigned to the Personnel Security Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-14: PERSONNEL SECURITY FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PS-1	**Policy and Procedures**		x	x	x
PS-2	**Position Risk Designation**		x	x	x
PS-3	**Personnel Screening**		x	x	x
PS-3(1)	CLASSIFIED INFORMATION				
PS-3(2)	FORMAL INDOCTRINATION				
PS-3(3)	INFORMATION REQUIRING SPECIAL PROTECTIVE MEASURES				
PS-3(4)	CITIZENSHIP REQUIREMENTS				
PS-4	**Personnel Termination**		x	x	x
PS-4(1)	POST-EMPLOYMENT REQUIREMENTS				
PS-4(2)	AUTOMATED ACTIONS				x
PS-5	**Personnel Transfer**		x	x	x
PS-6	**Access Agreements**	x	x	x	x
PS-6(1)	INFORMATION REQUIRING SPECIAL PROTECTION	W: Incorporated into PS-3.			
PS-6(2)	CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION				
PS-6(3)	POST-EMPLOYMENT REQUIREMENTS				
PS-7	**External Personnel Security**		x	x	x
PS-8	**Personnel Sanctions**		x	x	x
PS-9	**Position Descriptions**		x	x	x

3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY FAMILY

Table 3-15 provides a summary of the controls and control enhancements assigned to the Personally Identifiable Information Processing and Transparency Family. The controls are allocated to the privacy control baseline in accordance with the selection criteria defined in Section 2.2. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-15: PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PT-1	**Policy and Procedures**	x	**Personally Identifiable Information Processing and Transparency controls are not allocated to the security control baselines.** **Privacy baseline controls are selected based on the selection criteria defined in Section 2.2.**		
PT-2	**Authority to Process Personally Identifiable Information**	x			
PT-2(1)	DATA TAGGING				
PT-2(2)	AUTOMATION				
PT-3	**Personally Identifiable Information Processing Purposes**	x			
PT-3(1)	DATA TAGGING				
PT-3(2)	AUTOMATION				
PT-4	**Consent**	x			
PT-4(1)	TAILORED CONSENT				
PT-4(2)	JUST-IN-TIME CONSENT				
PT-4(3)	REVOCATION				
PT-5	**Privacy Notice**	x			
PT-5(1)	JUST-IN-TIME NOTICE				
PT-5(2)	PRIVACY ACT STATEMENTS	x			
PT-6	**System of Records Notice**	x			
PT-6(1)	ROUTINE USES	x			
PT-6(2)	EXEMPTION RULES	x			
PT-7	**Specific Categories of Personally Identifiable Information**	x			
PT-7(1)	SOCIAL SECURITY NUMBERS	x			
PT-7(2)	FIRST AMENDMENT INFORMATION	x			
PT-8	**Computer Matching Requirements**	x			

3.16 RISK ASSESSMENT FAMILY

Table 3-16 provides a summary of the controls and control enhancements assigned to the Risk Assessment Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-16: RISK ASSESSMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
RA-1	**Policy and Procedures**	x	x	x	x
RA-2	**Security Categorization**		x	x	x
RA-2(1)	IMPACT-LEVEL PRIORITIZATION				
RA-3	**Risk Assessment**	x	x	x	x
RA-3(1)	SUPPLY CHAIN RISK ASSESSMENT		x	x	x
RA-3(2)	USE OF ALL-SOURCE INTELLIGENCE				
RA-3(3)	DYNAMIC THREAT AWARENESS				
RA-3(4)	PREDICTIVE CYBER ANALYTICS				
RA-4	**Risk Assessment Update**	W: Incorporated into RA-3.			
RA-5	**Vulnerability Monitoring and Scanning**		x	x	x
RA-5(1)	UPDATE TOOL CAPABILITY	W: Incorporated into RA-5.			
RA-5(2)	UPDATE VULNERABILITIES TO BE SCANNED		x	x	x
RA-5(3)	BREADTH AND DEPTH OF COVERAGE				
RA-5(4)	DISCOVERABLE INFORMATION				x
RA-5(5)	PRIVILEGED ACCESS			x	x
RA-5(6)	AUTOMATED TREND ANALYSES				
RA-5(7)	AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS	W: Incorporated into CM-8.			
RA-5(8)	REVIEW HISTORIC AUDIT LOGS				
RA-5(9)	PENETRATION TESTING AND ANALYSES	W: Incorporated into CA-8.			
RA-5(10)	CORRELATE SCANNING INFORMATION				
RA-5(11)	PUBLIC DISCLOSURE PROGRAM		x	x	x
RA-6	**Technical Surveillance Countermeasures Survey**				
RA-7	**Risk Response**	x	x	x	x
RA-8	**Privacy Impact Assessments**	x			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
RA-9	**Criticality Analysis**			x	x
RA-10	**Threat Hunting**				

3.17 SYSTEM AND SERVICES ACQUISITION FAMILY

Table 3-17 provides a summary of the controls and control enhancements assigned to the System and Services Acquisition Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-17: SYSTEM AND SERVICES ACQUISITION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SA-1	**Policy and Procedures**	x	x	x	x
SA-2	**Allocation of Resources**	x	x	x	x
SA-3	**System Development Life Cycle**	x	x	x	x
SA-3(1)	MANAGE PREPRODUCTION ENVIRONMENT				
SA-3(2)	USE OF LIVE OR OPERATIONAL DATA				
SA-3(3)	TECHNOLOGY REFRESH				
SA-4	**Acquisition Process**	x	x	x	x
SA-4(1)	FUNCTIONAL PROPERTIES OF CONTROLS			x	x
SA-4(2)	DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS			x	x
SA-4(3)	DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES				
SA-4(4)	ASSIGNMENT OF COMPONENTS TO SYSTEMS	W: Incorporated into CM-8(9).			
SA-4(5)	SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS				x
SA-4(6)	USE OF INFORMATION ASSURANCE PRODUCTS				
SA-4(7)	NIAP-APPROVED PROTECTION PROFILES				
SA-4(8)	CONTINUOUS MONITORING PLAN FOR CONTROLS				
SA-4(9)	FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE			x	x
SA-4(10)	USE OF APPROVED PIV PRODUCTS		x	x	x
SA-4(11)	SYSTEM OF RECORDS				
SA-4(12)	DATA OWNERSHIP				
SA-5	**System Documentation**		x	x	x
SA-5(1)	FUNCTIONAL PROPERTIES OF SECURITY CONTROLS	W: Incorporated into SA-4(1).			
SA-5(2)	SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES	W: Incorporated into SA-4(2).			
SA-5(3)	HIGH-LEVEL DESIGN	W: Incorporated into SA-4(2).			
SA-5(4)	LOW-LEVEL DESIGN	W: Incorporated into SA-4(2).			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SA-5(5)	SOURCE CODE	W: Incorporated into SA-4(2).			
SA-6	**Software Usage Restrictions**	W: Incorporated into CM-10 and SI-7.			
SA-7	**User-installed Software**	W: Incorporated into CM-11 and SI-7.			
SA-8	**Security and Privacy Engineering Principles**		x	x	x
SA-8(1)	CLEAR ABSTRACTIONS				
SA-8(2)	LEAST COMMON MECHANISM				
SA-8(3)	MODULARITY AND LAYERING				
SA-8(4)	PARTIALLY ORDERED DEPENDENCIES				
SA-8(5)	EFFICIENTLY MEDIATED ACCESS				
SA-8(6)	MINIMIZED SHARING				
SA-8(7)	REDUCED COMPLEXITY				
SA-8(8)	SECURE EVOLVABILITY				
SA-8(9)	TRUSTED COMPONENTS				
SA-8(10)	HIERARCHICAL TRUST				
SA-8(11)	INVERSE MODIFICATION THRESHOLD				
SA-8(12)	HIERARCHICAL PROTECTION				
SA-8(13)	MINIMIZED SECURITY ELEMENTS				
SA-8(14)	LEAST PRIVILEGE				
SA-8(15)	PREDICATE PERMISSION				
SA-8(16)	SELF-RELIANT TRUSTWORTHINESS				
SA-8(17)	SECURE DISTRIBUTED COMPOSITION				
SA-8(18)	TRUSTED COMMUNICATIONS CHANNELS				
SA-8(19)	CONTINUOUS PROTECTION				
SA-8(20)	SECURE METADATA MANAGEMENT				
SA-8(21)	SELF-ANALYSIS				
SA-8(22)	ACCOUNTABILITY AND TRACEABILITY				
SA-8(23)	SECURE DEFAULTS				
SA-8(24)	SECURE FAILURE AND RECOVERY				
SA-8(25)	ECONOMIC SECURITY				
SA-8(26)	PERFORMANCE SECURITY				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SA-8(27)	HUMAN FACTORED SECURITY				
SA-8(28)	ACCEPTABLE SECURITY				
SA-8(29)	REPEATABLE AND DOCUMENTED PROCEDURES				
SA-8(30)	PROCEDURAL RIGOR				
SA-8(31)	SECURE SYSTEM MODIFICATION				
SA-8(32)	SUFFICIENT DOCUMENTATION				
SA-8(33)	MINIMIZATION	x			
SA-9	**External System Services**	x	x	x	x
SA-9(1)	RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS				
SA-9(2)	IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES			x	x
SA-9(3)	ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS				
SA-9(4)	CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS				
SA-9(5)	PROCESSING, STORAGE, AND SERVICE LOCATION				
SA-9(6)	ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS				
SA-9(7)	ORGANIZATION-CONTROLLED INTEGRITY CHECKING				
SA-9(8)	PROCESSING AND STORAGE LOCATION — U.S. JURISDICTION				
SA-10	**Developer Configuration Management**			x	x
SA-10(1)	SOFTWARE AND FIRMWARE INTEGRITY VERIFICATION				
SA-10(2)	ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES				
SA-10(3)	HARDWARE INTEGRITY VERIFICATION				
SA-10(4)	TRUSTED GENERATION				
SA-10(5)	MAPPING INTEGRITY FOR VERSION CONTROL				
SA-10(6)	TRUSTED DISTRIBUTION				
SA-10(7)	SECURITY AND PRIVACY REPRESENTATIVES				
SA-11	**Developer Testing and Evaluation**	x		x	x
SA-11(1)	STATIC CODE ANALYSIS				
SA-11(2)	THREAT MODELING AND VULNERABILITY ANALYSES				
SA-11(3)	INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE				
SA-11(4)	MANUAL CODE REVIEWS				
SA-11(5)	PENETRATION TESTING				
SA-11(6)	ATTACK SURFACE REVIEWS				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SA-11(7)	VERIFY SCOPE OF TESTING AND EVALUATION				
SA-11(8)	DYNAMIC CODE ANALYSIS				
SA-11(9)	INTERACTIVE APPLICATION SECURITY TESTING				
SA-12	**Supply Chain Protection**	W: Moved to SR Family.			
SA-12(1)	ACQUISITION STRATEGIES / TOOLS / METHODS	W: Moved to SR-5.			
SA-12(2)	SUPPLIER REVIEWS	W: Moved to SR-6.			
SA-12(3)	TRUSTED SHIPPING AND WAREHOUSING	W: Incorporated into SR-3.			
SA-12(4)	DIVERSITY OF SUPPLIERS	W: Moved to SR-3(1).			
SA-12(5)	LIMITATION OF HARM	W: Moved to SR-3(2).			
SA-12(6)	MINIMIZING PROCUREMENT TIME	W: Incorporated into SR-5(1).			
SA-12(7)	ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE	W: Moved to SR-5(2).			
SA-12(8)	USE OF ALL-SOURCE INTELLIGENCE	W: Incorporated into RA-3(2).			
SA-12(9)	OPERATIONS SECURITY	W: Moved to SR-7.			
SA-12(10)	VALIDATE AS GENUINE AND NOT ALTERED	W: Moved to SR-4(3).			
SA-12(11)	PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS	W: Moved to SR-6(1).			
SA-12(12)	INTER-ORGANIZATIONAL AGREEMENTS	W: Moved to SR-8.			
SA-12(13)	CRITICAL INFORMATION SYSTEM COMPONENTS	W: Incorporated into MA-6 and RA-9.			
SA-12(14)	IDENTITY AND TRACEABILITY	W: Moved to SR-4(1) and SR-4(2).			
SA-12(15)	PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES	W: Incorporated into SR-3.			
SA-13	**Trustworthiness**	W: Incorporated into SA-8.			
SA-14	**Criticality Analysis**	W: Incorporated into RA-9.			
SA-14(1)	CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING	W: Incorporated into SA-20.			
SA-15	**Development Process, Standards, and Tools**			x	x
SA-15(1)	QUALITY METRICS				
SA-15(2)	SECURITY AND PRIVACY TRACKING TOOLS				
SA-15(3)	CRITICALITY ANALYSIS			x	x
SA-15(4)	THREAT MODELING AND VULNERABILITY ANALYSIS	W: Incorporated into SA-11(2).			
SA-15(5)	ATTACK SURFACE REDUCTION				
SA-15(6)	CONTINUOUS IMPROVEMENT				
SA-15(7)	AUTOMATED VULNERABILITY ANALYSIS				
SA-15(8)	REUSE OF THREAT AND VULNERABILITY INFORMATION				
SA-15(9)	USE OF LIVE DATA	W: Incorporated into SA-3(2).			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SA-15(10)	INCIDENT RESPONSE PLAN				
SA-15(11)	ARCHIVE SYSTEM OR COMPONENT				
SA-15(12)	MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION				
SA-16	**Developer-provided Training**				x
SA-17	**Developer Security and Privacy Architecture and Design**				x
SA-17(1)	FORMAL POLICY MODEL				
SA-17(2)	SECURITY-RELEVANT COMPONENTS				
SA-17(3)	FORMAL CORRESPONDENCE				
SA-17(4)	INFORMAL CORRESPONDENCE				
SA-17(5)	CONCEPTUALLY SIMPLE DESIGN				
SA-17(6)	STRUCTURE FOR TESTING				
SA-17(7)	STRUCTURE FOR LEAST PRIVILEGE				
SA-17(8)	ORCHESTRATION				
SA-17(9)	DESIGN DIVERSITY				
SA-18	**Tamper Resistance and Detection**	W: Moved to SR-9.			
SA-18(1)	MULTIPLE PHASES OF SYSTEM DEVELOPMENT LIFE CYCLE	W: Moved to SR-9(1).			
SA-18(2)	INSPECTION OF SYSTEMS OR COMPONENTS	W: Moved to SR-10.			
SA-19	**Component Authenticity**	W: Moved to SR-11.			
SA-19(1)	ANTI-COUNTERFEIT TRAINING	W: Moved to SR-11(1).			
SA-19(2)	CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR	W: Moved to SR-11(2).			
SA-19(3)	COMPONENT DISPOSAL	W: Moved to SR-12.			
SA-19(4)	ANTI-COUNTERFEIT SCANNING	W: Moved to SR-11(3).			
SA-20	**Customized Development of Critical Components**				
SA-21	**Developer Screening**				x
SA-21(1)	VALIDATION OF SCREENING	W: Incorporated into SA-21.			
SA-22	**Unsupported System Components**		x	x	x
SA-22(1)	ALTERNATIVE SOURCES FOR CONTINUED SUPPORT	W: Incorporated into SA-22.			
SA-23	**Specialization**				

3.18 SYSTEM AND COMMUNICATIONS PROTECTION FAMILY

Table 3-18 provides a summary of the controls and control enhancements assigned to the System and Communications Protection Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-18: SYSTEM AND COMMUNICATIONS PROTECTION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-1	**Policy and Procedures**		x	x	x
SC-2	**Separation of System and User Functionality**			x	x
SC-2(1)	INTERFACES FOR NON-PRIVILEGED USERS				
SC-2(2)	DISASSOCIABILITY				
SC-3	**Security Function Isolation**				x
SC-3(1)	HARDWARE SEPARATION				
SC-3(2)	ACCESS AND FLOW CONTROL FUNCTIONS				
SC-3(3)	MINIMIZE NONSECURITY FUNCTIONALITY				
SC-3(4)	MODULE COUPLING AND COHESIVENESS				
SC-3(5)	LAYERED STRUCTURES				
SC-4	**Information in Shared System Resources**			x	x
SC-4(1)	SECURITY LEVELS	W: Incorporated into SC-4.			
SC-4(2)	MULTILEVEL OR PERIODS PROCESSING				
SC-5	**Denial-of-service Protection**		x	x	x
SC-5(1)	RESTRICT ABILITY TO ATTACK OTHER SYSTEMS				
SC-5(2)	CAPACITY, BANDWIDTH, AND REDUNDANCY				
SC-5(3)	DETECTION AND MONITORING				
SC-6	**Resource Availability**				
SC-7	**Boundary Protection**		x	x	x
SC-7(1)	PHYSICALLY SEPARATED SUBNETWORKS	W: Incorporated into SC-7.			
SC-7(2)	PUBLIC ACCESS	W: Incorporated into SC-7.			
SC-7(3)	ACCESS POINTS			x	x
SC-7(4)	EXTERNAL TELECOMMUNICATIONS SERVICES			x	x
SC-7(5)	DENY BY DEFAULT — ALLOW BY EXCEPTION			x	x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-7(6)	RESPONSE TO RECOGNIZED FAILURES	W: Incorporated into SC-7(18).			
SC-7(7)	SPLIT TUNNELING FOR REMOTE DEVICES			x	x
SC-7(8)	ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS			x	x
SC-7(9)	RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC				
SC-7(10)	PREVENT EXFILTRATION				
SC-7(11)	RESTRICT INCOMING COMMUNICATIONS TRAFFIC				
SC-7(12)	HOST-BASED PROTECTION				
SC-7(13)	ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS				
SC-7(14)	PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS				
SC-7(15)	NETWORKED PRIVILEGED ACCESSES				
SC-7(16)	PREVENT DISCOVERY OF SYSTEM COMPONENTS				
SC-7(17)	AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS				
SC-7(18)	FAIL SECURE				x
SC-7(19)	BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS				
SC-7(20)	DYNAMIC ISOLATION AND SEGREGATION				
SC-7(21)	ISOLATION OF SYSTEM COMPONENTS				x
SC-7(22)	SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS				
SC-7(23)	DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE				
SC-7(24)	PERSONALLY IDENTIFIABLE INFORMATION	x			
SC-7(25)	UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS				
SC-7(26)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS				
SC-7(27)	UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS				
SC-7(28)	CONNECTIONS TO PUBLIC NETWORKS				
SC-7(29)	SEPARATE SUBNETS TO ISOLATE FUNCTIONS				
SC-8	**Transmission Confidentiality and Integrity**			x	x
SC-8(1)	CRYPTOGRAPHIC PROTECTION			x	x
SC-8(2)	PRE- AND POST-TRANSMISSION HANDLING				
SC-8(3)	CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS				
SC-8(4)	CONCEAL OR RANDOMIZE COMMUNICATIONS				
SC-8(5)	PROTECTED DISTRIBUTION SYSTEM				
SC-9	**Transmission Confidentiality**	W: Incorporated into SC-8.			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-10	**Network Disconnect**			x	x
SC-11	**Trusted Path**				
SC-11(1)	IRREFUTABLE COMMUNICATIONS PATH				
SC-12	**Cryptographic Key Establishment and Management**		x	x	x
SC-12(1)	AVAILABILITY				x
SC-12(2)	SYMMETRIC KEYS				
SC-12(3)	ASYMMETRIC KEYS				
SC-12(4)	PKI CERTIFICATES	W: Incorporated into SC-12(3).			
SC-12(5)	PKI CERTIFICATES / HARDWARE TOKENS	W: Incorporated into SC-12(3).			
SC-12(6)	PHYSICAL CONTROL OF KEYS				
SC-13	**Cryptographic Protection**		x	x	x
SC-13(1)	FIPS-VALIDATED CRYPTOGRAPHY	W: Incorporated into SC-13.			
SC-13(2)	NSA-APPROVED CRYPTOGRAPHY	W: Incorporated into SC-13.			
SC-13(3)	INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS	W: Incorporated into SC-13.			
SC-13(4)	DIGITAL SIGNATURES	W: Incorporated into SC-13.			
SC-14	**Public Access Protections**	W: Incorporated into AC-2,AC-3,AC-5,AC-6,SI-3,SI-4, SI-5,SI-7, and SI-10.			
SC-15	**Collaborative Computing Devices and Applications**		x	x	x
SC-15(1)	PHYSICAL OR LOGICAL DISCONNECT				
SC-15(2)	BLOCKING INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	W: Incorporated into SC-7.			
SC-15(3)	DISABLING AND REMOVAL IN SECURE WORK AREAS				
SC-15(4)	EXPLICITLY INDICATE CURRENT PARTICIPANTS				
SC-16	**Transmission of Security and Privacy Attributes**				
SC-16(1)	INTEGRITY VERIFICATION				
SC-16(2)	ANTI-SPOOFING MECHANISMS				
SC-16(3)	CRYPTOGRAPHIC BINDING				
SC-17	**Public Key Infrastructure Certificates**			x	x
SC-18	**Mobile Code**			x	x
SC-18(1)	IDENTIFY UNACCEPTABLE CODE AND TAKE CORRECTIVE ACTIONS				
SC-18(2)	ACQUISITION, DEVELOPMENT, AND USE				
SC-18(3)	PREVENT DOWNLOADING AND EXECUTION				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-18(4)	PREVENT AUTOMATIC EXECUTION				
SC-18(5)	ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS				
SC-19	**Voice Over Internet Protocol**	W: Technology-specific; addressed as any other technology or protocol.			
SC-20	**Secure Name/Address Resolution Service (Authoritative Source)**		x	x	x
SC-20(1)	CHILD SUBSPACES	W: Incorporated into SC-20.			
SC-20(2)	DATA ORIGIN AND INTEGRITY				
SC-21	**Secure Name/Address Resolution Service (Recursive or Caching Resolver)**		x	x	x
SC-21(1)	DATA ORIGIN AND INTEGRITY	W: Incorporated into SC-21.			
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**		x	x	x
SC-23	**Session Authenticity**			x	x
SC-23(1)	INVALIDATE SESSION IDENTIFIERS AT LOGOUT				
SC-23(2)	USER-INITIATED LOGOUTS AND MESSAGE DISPLAYS	W: Incorporated into AC-12(1).			
SC-23(3)	UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS				
SC-23(4)	UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION	W: Incorporated into SC-23(3).			
SC-23(5)	ALLOWED CERTIFICATE AUTHORITIES				
SC-24	**Fail in Known State**				x
SC-25	**Thin Nodes**				
SC-26	**Decoys**				
SC-26(1)	DETECTION OF MALICIOUS CODE	W: Incorporated into SC-35.			
SC-27	**Platform-independent Applications**				
SC-28	**Protection of Information at Rest**			x	x
SC-28(1)	CRYPTOGRAPHIC PROTECTION			x	x
SC-28(2)	OFFLINE STORAGE				
SC-28(3)	CRYPTOGRAPHIC KEYS				
SC-29	**Heterogeneity**				
SC-29(1)	VIRTUALIZATION TECHNIQUES				
SC-30	**Concealment and Misdirection**				
SC-30(1)	VIRTUALIZATION TECHNIQUES	W: Incorporated into SC-29(1).			
SC-30(2)	RANDOMNESS				
SC-30(3)	CHANGE PROCESSING AND STORAGE LOCATIONS				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-30(4)	MISLEADING INFORMATION				
SC-30(5)	CONCEALMENT OF SYSTEM COMPONENTS				
SC-31	**Covert Channel Analysis**				
SC-31(1)	TEST COVERT CHANNELS FOR EXPLOITABILITY				
SC-31(2)	MAXIMUM BANDWIDTH				
SC-31(3)	MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS				
SC-32	**System Partitioning**				
SC-32(1)	SEPARATE PHYSICAL DOMAINS FOR PRIVILEGED FUNCTIONS				
SC-33	**Transmission Preparation Integrity**	W: Incorporated into SC-8.			
SC-34	**Non-modifiable Executable Programs**				
SC-34(1)	NO WRITABLE STORAGE				
SC-34(2)	INTEGRITY PROTECTION ON READ-ONLY MEDIA				
SC-34(3)	HARDWARE-BASED PROTECTION	W: Moved to SC-51.			
SC-35	**External Malicious Code Identification**				
SC-36	**Distributed Processing and Storage**				
SC-36(1)	POLLING TECHNIQUES				
SC-36(2)	SYNCHRONIZATION				
SC-37	**Out-of-band Channels**				
SC-37(1)	ENSURE DELIVERY AND TRANSMISSION				
SC-38	**Operations Security**				
SC-39	**Process Isolation**		x	x	x
SC-39(1)	HARDWARE SEPARATION				
SC-39(2)	SEPARATE EXECUTION DOMAIN PER THREAD				
SC-40	**Wireless Link Protection**				
SC-40(1)	ELECTROMAGNETIC INTERFERENCE				
SC-40(2)	REDUCE DETECTION POTENTIAL				
SC-40(3)	IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION				
SC-40(4)	SIGNAL PARAMETER IDENTIFICATION				
SC-41	**Port and I/O Device Access**				
SC-42	**Sensor Capability and Data**				
SC-42(1)	REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-42(2)	AUTHORIZED USE				
SC-42(3)	PROHIBIT USE OF DEVICES	W: Incorporated into SC-42.			
SC-42(4)	NOTICE OF COLLECTION				
SC-42(5)	COLLECTION MINIMIZATION				
SC-43	**Usage Restrictions**				
SC-44	**Detonation Chambers**				
SC-45	**System Time Synchronization**				
SC-45(1)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE				
SC-45(2)	SECONDARY AUTHORITATIVE TIME SOURCE				
SC-46	**Cross Domain Policy Enforcement**				
SC-47	**Alternate Communications Paths**				
SC-48	**Sensor Relocation**				
SC-48(1)	DYNAMIC RELOCATION OF SENSORS OR MONITORING CAPABILITIES				
SC-49	**Hardware-enforced Separation and Policy Enforcement**				
SC-50	**Software-enforced Separation and Policy Enforcement**				
SC-51	**Hardware-based Protection**				

3.19 SYSTEM AND INFORMATION INTEGRITY FAMILY

Table 3-19 provides a summary of the controls and control enhancements assigned to the System and Information Integrity Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-19: SYSTEM AND INFORMATION INTEGRITY FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SI-1	**Policy and Procedures**	x	x	x	x
SI-2	**Flaw Remediation**		x	x	x
SI-2(1)	CENTRAL MANAGEMENT	W: Incorporated into PL-9.			
SI-2(2)	AUTOMATED FLAW REMEDIATION STATUS			x	x
SI-2(3)	TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS				
SI-2(4)	AUTOMATED PATCH MANAGEMENT TOOLS				
SI-2(5)	AUTOMATIC SOFTWARE AND FIRMWARE UPDATES				
SI-2(6)	REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE AND FIRMWARE				
SI-3	**Malicious Code Protection**		x	x	x
SI-3(1)	CENTRAL MANAGEMENT	W: Incorporated into PL-9.			
SI-3(2)	AUTOMATIC UPDATES	W: Incorporated into SI-3.			
SI-3(3)	NON-PRIVILEGED USERS	W: Incorporated into AC-6(10).			
SI-3(4)	UPDATES ONLY BY PRIVILEGED USERS				
SI-3(5)	PORTABLE STORAGE DEVICES	W: Incorporated into MP-7.			
SI-3(6)	TESTING AND VERIFICATION				
SI-3(7)	NONSIGNATURE-BASED DETECTION	W: Incorporated into SI-3.			
SI-3(8)	DETECT UNAUTHORIZED COMMANDS				
SI-3(9)	AUTHENTICATE REMOTE COMMANDS	W: Moved to AC-17(10).			
SI-3(10)	MALICIOUS CODE ANALYSIS				
SI-4	**System Monitoring**		x	x	x
SI-4(1)	SYSTEM-WIDE INTRUSION DETECTION SYSTEM				
SI-4(2)	AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS			x	x
SI-4(3)	AUTOMATED TOOL AND MECHANISM INTEGRATION				
SI-4(4)	INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC			x	x
SI-4(5)	SYSTEM-GENERATED ALERTS			x	x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SI-4(6)	RESTRICT NON-PRIVILEGED USERS	W: Incorporated into AC-6(10).			
SI-4(7)	AUTOMATED RESPONSE TO SUSPICIOUS EVENTS				
SI-4(8)	PROTECTION OF MONITORING INFORMATION	W: Incorporated into SI-4.			
SI-4(9)	TESTING OF MONITORING TOOLS AND MECHANISMS				
SI-4(10)	VISIBILITY OF ENCRYPTED COMMUNICATIONS				x
SI-4(11)	ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES				
SI-4(12)	AUTOMATED ORGANIZATION-GENERATED ALERTS				x
SI-4(13)	ANALYZE TRAFFIC AND EVENT PATTERNS				
SI-4(14)	WIRELESS INTRUSION DETECTION				x
SI-4(15)	WIRELESS TO WIRELINE COMMUNICATIONS				
SI-4(16)	CORRELATE MONITORING INFORMATION				
SI-4(17)	INTEGRATED SITUATIONAL AWARENESS				
SI-4(18)	ANALYZE TRAFFIC AND COVERT EXFILTRATION				
SI-4(19)	RISK FOR INDIVIDUALS				
SI-4(20)	PRIVILEGED USERS				x
SI-4(21)	PROBATIONARY PERIODS				
SI-4(22)	UNAUTHORIZED NETWORK SERVICES				x
SI-4(23)	HOST-BASED DEVICES				
SI-4(24)	INDICATORS OF COMPROMISE				
SI-4(25)	OPTIMIZE NETWORK TRAFFIC ANALYSIS				
SI-5	**Security Alerts, Advisories, and Directives**		x	x	x
SI-5(1)	AUTOMATED ALERTS AND ADVISORIES				x
SI-6	**Security and Privacy Function Verification**				x
SI-6(1)	NOTIFICATION OF FAILED SECURITY TESTS	W: Incorporated into SI-6.			
SI-6(2)	AUTOMATION SUPPORT FOR DISTRIBUTED TESTING				
SI-6(3)	REPORT VERIFICATION RESULTS				
SI-7	**Software, Firmware, and Information Integrity**			x	x
SI-7(1)	INTEGRITY CHECKS			x	x
SI-7(2)	AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS				x
SI-7(3)	CENTRALLY MANAGED INTEGRITY TOOLS				
SI-7(4)	TAMPER-EVIDENT PACKAGING	W: Incorporated into SR-9.			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SI-7(5)	AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS				x
SI-7(6)	CRYPTOGRAPHIC PROTECTION				
SI-7(7)	INTEGRATION OF DETECTION AND RESPONSE			x	x
SI-7(8)	AUDITING CAPABILITY FOR SIGNIFICANT EVENTS				
SI-7(9)	VERIFY BOOT PROCESS				
SI-7(10)	PROTECTION OF BOOT FIRMWARE				
SI-7(11)	CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES	W: Moved to CM-7(6).			
SI-7(12)	INTEGRITY VERIFICATION				
SI-7(13)	CODE EXECUTION IN PROTECTED ENVIRONMENTS	W: Moved to CM-7(7).			
SI-7(14)	BINARY OR MACHINE EXECUTABLE CODE	W: Moved to CM-7(8).			
SI-7(15)	CODE AUTHENTICATION				x
SI-7(16)	TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION				
SI-7(17)	RUNTIME APPLICATION SELF-PROTECTION				
SI-8	**Spam Protection**			x	x
SI-8(1)	CENTRAL MANAGEMENT	W: Incorporated into PL-9.			
SI-8(2)	AUTOMATIC UPDATES			x	x
SI-8(3)	CONTINUOUS LEARNING CAPABILITY				
SI-9	**Information Input Restrictions**	W: Incorporated into AC-2, AC-3, AC-5, and AC-6.			
SI-10	**Information Input Validation**			x	x
SI-10(1)	MANUAL OVERRIDE CAPABILITY				
SI-10(2)	REVIEW AND RESOLVE ERRORS				
SI-10(3)	PREDICTABLE BEHAVIOR				
SI-10(4)	TIMING INTERACTIONS				
SI-10(5)	RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS				
SI-10(6)	INJECTION PREVENTION				
SI-11	**Error Handling**			x	x
SI-12	**Information Management and Retention**	x	x	x	x
SI-12(1)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	x			
SI-12(2)	MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH	x			
SI-12(3)	INFORMATION DISPOSAL	x			
SI-13	**Predictable Failure Prevention**				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SI-13(1)	TRANSFERRING COMPONENT RESPONSIBILITIES				
SI-13(2)	TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION	W: Incorporated into SI-7(16).			
SI-13(3)	MANUAL TRANSFER BETWEEN COMPONENTS				
SI-13(4)	STANDBY COMPONENT INSTALLATION AND NOTIFICATION				
SI-13(5)	FAILOVER CAPABILITY				
SI-14	**Non-persistence**				
SI-14(1)	REFRESH FROM TRUSTED SOURCES				
SI-14(2)	NON-PERSISTENT INFORMATION				
SI-14(3)	NON-PERSISTENT CONNECTIVITY				
SI-15	**Information Output Filtering**				
SI-16	**Memory Protection**			x	x
SI-17	**Fail-safe Procedures**				
SI-18	**Personally Identifiable Information Quality Operations**	x			
SI-18(1)	AUTOMATION SUPPORT				
SI-18(2)	DATA TAGS				
SI-18(3)	COLLECTION				
SI-18(4)	INDIVIDUAL REQUESTS	x			
SI-18(5)	NOTICE OF CORRECTION OR DELETION				
SI-19	**De-identification**	x			
SI-19(1)	COLLECTION				
SI-19(2)	ARCHIVING				
SI-19(3)	RELEASE				
SI-19(4)	REMOVAL, MASKING, ENCRYPTION, HASHING, OR REPLACEMENT OF DIRECT IDENTIFIERS				
SI-19(5)	STATISTICAL DISCLOSURE CONTROL				
SI-19(6)	DIFFERENTIAL PRIVACY				
SI-19(7)	VALIDATED ALGORITHMS AND SOFTWARE				
SI-19(8)	MOTIVATED INTRUDER				
SI-20	**Tainting**				
SI-21	**Information Refresh**				
SI-22	**Information Diversity**				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SI-23	**Information Fragmentation**				

3.20 SUPPLY CHAIN RISK MANAGEMENT FAMILY

Table 3-20 provides a summary of the controls and control enhancements assigned to the Supply Chain Risk Management Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-20: SUPPLY CHAIN RISK MANAGEMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SR-1	**Policy and Procedures**		x	x	x
SR-2	**Supply Chain Risk Management Plan**		x	x	x
SR-2(1)	ESTABLISH SCRM TEAM		x	x	x
SR-3	**Supply Chain Controls and Processes**		x	x	x
SR-3(1)	DIVERSE SUPPLY BASE				
SR-3(2)	LIMITATION OF HARM				
SR-3(3)	SUB-TIER FLOW DOWN				
SR-4	**Provenance**				
SR-4(1)	IDENTITY				
SR-4(2)	TRACK AND TRACE				
SR-4(3)	VALIDATE AS GENUINE AND NOT ALTERED				
SR-4(4)	SUPPLY CHAIN INTEGRITY — PEDIGREE				
SR-5	**Acquisition Strategies, Tools, and Methods**		x	x	x
SR-5(1)	ADEQUATE SUPPLY				
SR-5(2)	ASSESSMENTS PRIOR TO SELECTION, ACCEPTANCE, MODIFICATION, OR UPDATE				
SR-6	**Supplier Assessments and Reviews**			x	x
SR-6(1)	TESTING AND ANALYSIS				
SR-7	**Supply Chain Operations Security**				
SR-8	**Notification Agreements**		x	x	x
SR-9	**Tamper Resistance and Detection**				x
SR-9(1)	MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE				x
SR-10	**Inspection of Systems or Components**		x	x	x
SR-11	**Component Authenticity**		x	x	x
SR-11(1)	ANTI-COUNTERFEIT TRAINING		x	x	x

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SR-11(2)	CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR		x	x	x
SR-11(3)	ANTI-COUNTERFEIT SCANNING				
SR-12	**Component Disposal**		x	x	x