SecureHIT Security and Privacy Control Collaboration Index

This collaboration index supports information security and privacy program collaboration to help ensure that the objectives of both disciplines are met and that risks are appropriately managed. It is an optional tool for information security and privacy programs to identify the degree of collaboration needed between security and privacy programs with respect to the selection and/or implementation of controls in NIST Special Publication (SP) 800-53, Revision 5. There may be circumstances where the selection and/or implementation of a control or control enhancement affects the ability of a security or privacy program to achieve its objectives and manage its respective risks. While the discussion section may highlight specific security and/or privacy considerations, they are not exhaustive.

ACCESS CONTROL FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
AC-1	**Policy and Procedures**	SP
AC-2	**Account Management**	S
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT	S
AC-2(2)	AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT	S
AC-2(3)	DISABLE ACCOUNTS	S
AC-2(4)	AUTOMATED AUDIT ACTIONS	S
AC-2(5)	INACTIVITY LOGOUT	S
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT	S
AC-2(7)	PRIVILEGED USER ACCOUNTS	S
AC-2(8)	DYNAMIC ACCOUNT MANAGEMENT	S
AC-2(9)	RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS	S
AC-2(10)	SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE	
AC-2(11)	USAGE CONDITIONS	S
AC-2(12)	ACCOUNT MONITORING FOR ATYPICAL USAGE	S
AC-2(13)	DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS	S
AC-3	**Access Enforcement**	S
AC-3(1)	RESTRICTED ACCESS TO PRIVILEGED FUNCTION	
AC-3(2)	DUAL AUTHORIZATION	S
AC-3(3)	MANDATORY ACCESS CONTROL	S
AC-3(4)	DISCRETIONARY ACCESS CONTROL	S
AC-3(5)	SECURITY-RELEVANT INFORMATION	S
AC-3(6)	PROTECTION OF USER AND SYSTEM INFORMATION	
AC-3(7)	ROLE-BASED ACCESS CONTROL	S
AC-3(8)	REVOCATION OF ACCESS AUTHORIZATIONS	S
AC-3(9)	CONTROLLED RELEASE	SP
AC-3(10)	AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS	S
AC-3(11)	RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES	SP
AC-3(12)	ASSERT AND ENFORCE APPLICATION ACCESS	S
AC-3(13)	ATTRIBUTE-BASED ACCESS CONTROL	S

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
AC-3(14)	INDIVIDUAL ACCESS	SP
AC-3(15)	DISCRETIONARY AND MANDATORY ACCESS CONTROL	S
AC-4	**Information Flow Enforcement**	S
AC-4(1)	OBJECT SECURITY AND PRIVACY ATTRIBUTES	S
AC-4(2)	PROCESSING DOMAINS	S
AC-4(3)	DYNAMIC INFORMATION FLOW CONTROL	S
AC-4(4)	FLOW CONTROL OF ENCRYPTED INFORMATION	S
AC-4(5)	EMBEDDED DATA TYPES	S
AC-4(6)	METADATA	S
AC-4(7)	ONE-WAY FLOW MECHANISMS	S
AC-4(8)	SECURITY AND PRIVACY POLICY FILTERS	S
AC-4(9)	HUMAN REVIEWS	SP
AC-4(10)	ENABLE AND DISABLE SECURITY OR PRIVACY POLICY FILTERS	S
AC-4(11)	CONFIGURATION OF SECURITY OR PRIVACY POLICY FILTERS	S
AC-4(12)	DATA TYPE IDENTIFIERS	S
AC-4(13)	DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS	S
AC-4(14)	SECURITY OR PRIVACY POLICY FILTER CONSTRAINTS	S
AC-4(15)	DETECTION OF UNSANCTIONED INFORMATION	S
AC-4(16)	INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS	
AC-4(17)	DOMAIN AUTHENTICATION	S
AC-4(18)	SECURITY ATTRIBUTE BINDING	
AC-4(19)	VALIDATION OF METADATA	S
AC-4(20)	APPROVED SOLUTIONS	S
AC-4(21)	PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS	S
AC-4(22)	ACCESS ONLY	S
AC-4(23)	MODIFY NON-RELEASABLE INFORMATION	S
AC-4(24)	INTERNAL NORMALIZED FORMAT	S
AC-4(25)	DATA SANITIZATION	S
AC-4(26)	AUDIT FILTERING ACTIONS	S
AC-4(27)	REDUNDANT/INDEPENDENT FILTERING MECHANISMS	S
AC-4(28)	LINEAR FILTER PIPELINES	S
AC-4(29)	FILTER ORCHESTRATION ENGINES	S
AC-4(30)	FILTER MECHANISMS USING MULTIPLE PROCESSES	S
AC-4(31)	FAILED CONTENT TRANSFER PREVENTION	S
AC-4(32)	PROCESS REQUIREMENTS FOR INFORMATION TRANSFER	S
AC-5	**Separation of Duties**	S
AC-6	**Least Privilege**	S
AC-6(1)	AUTHORIZE ACCESS TO SECURITY FUNCTIONS	S
AC-6(2)	NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	S
AC-6(3)	NETWORK ACCESS TO PRIVILEGED COMMANDS	S
AC-6(4)	SEPARATE PROCESSING DOMAINS	S
AC-6(5)	PRIVILEGED ACCOUNTS	S
AC-6(6)	PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS	S
AC-6(7)	REVIEW OF USER PRIVILEGES	S

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
AC-6(8)	PRIVILEGE LEVELS FOR CODE EXECUTION	S
AC-6(9)	LOG USE OF PRIVILEGED FUNCTIONS	S
AC-6(10)	PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	S
AC-7	**Unsuccessful Logon Attempts**	S
AC-7(1)	AUTOMATIC ACCOUNT LOCK	
AC-7(2)	PURGE OR WIPE MOBILE DEVICE	S
AC-7(3)	BIOMETRIC ATTEMPT LIMITING	S
AC-7(4)	USE OF ALTERNATE AUTHENTICATION FACTOR	S
AC-8	**System Use Notification**	SP
AC-9	**Previous Logon Notification**	S
AC-9(1)	UNSUCCESSFUL LOGONS	S
AC-9(2)	SUCCESSFUL AND UNSUCCESSFUL LOGONS	S
AC-9(3)	NOTIFICATION OF ACCOUNT CHANGES	S
AC-9(4)	ADDITIONAL LOGON INFORMATION	S
AC-10	**Concurrent Session Control**	S
AC-11	**Device Lock**	S
AC-11(1)	PATTERN-HIDING DISPLAYS	S
AC-12	**Session Termination**	S
AC-12(1)	USER-INITIATED LOGOUTS	S
AC-12(2)	TERMINATION MESSAGE	S
AC-12(3)	TIMEOUT WARNING MESSAGE	S
AC-13	**Supervision and Review-Access Control**	
AC-14	**Permitted Actions without Identification or Authentication**	S
AC-14(1)	NECESSARY USES	
AC-15	**Automated Marking**	
AC-16	**Security and Privacy Attributes**	SP
AC-16(1)	DYNAMIC ATTRIBUTE ASSOCIATION	S
AC-16(2)	ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS	SP
AC-16(3)	MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM	S
AC-16(4)	ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS	S
AC-16(5)	ATTRIBUTE DISPLAYS ON OBJECTS TO BE OUTPUT	
AC-16(6)	MAINTENANCE OF ATTRIBUTE ASSOCIATION	S
AC-16(7)	CONSISTENT ATTRIBUTE INTERPRETATION	S
AC-16(8)	ASSOCIATION TECHNIQUES AND TECHNOLOGIES	S
AC-16(9)	ATTRIBUTE REASSIGNMENT – REGRADING MECHANISMS	S
AC-16(10)	ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS	S
AC-17	**Remote Access**	S
AC-17(1)	MONITORING AND CONTROL	S
AC-17(2)	PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION	S
AC-17(3)	MANAGED ACCESS CONTROL POINTS	S
AC-17(4)	PRIVILEGED COMMANDS AND ACCESS	S
AC-17(5)	MONITORING FOR UNAUTHORIZED CONNECTIONS	
AC-17(6)	PROTECTION OF MECHANISM INFORMATION	S
AC-17(7)	ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS	

CONTROL NUMBER	**CONTROL NAME** CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
AC-17(8)	DISABLE NONSECURE NETWORK PROTOCOLS	
AC-17(9)	DISCONNECT OR DISABLE ACCESS	S
AC-17(10)	AUTHENTICATE REMOTE COMMANDS	S
AC-18	**Wireless Access**	S
AC-18(1)	AUTHENTICATION AND ENCRYPTION	S
AC-18(2)	MONITORING UNAUTHORIZED CONNECTIONS	
AC-18(3)	DISABLE WIRELESS NETWORKING	S
AC-18(4)	RESTRICT CONFIGURATIONS BY USERS	S
AC-18(5)	ANTENNAS AND TRANSMISSION POWER LEVELS	S
AC-19	**Access Control for Mobile Devices**	S
AC-19(1)	USE OF WRITABLE AND PORTABLE STORAGE DEVICES	
AC-19(2)	USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES	
AC-19(3)	USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER	
AC-19(4)	RESTRICTIONS FOR CLASSIFIED INFORMATION	S
AC-19(5)	FULL DEVICE OR CONTAINER-BASED ENCRYPTION	S
AC-20	**Use of External Systems**	SP
AC-20(1)	LIMITS ON AUTHORIZED USE	SP
AC-20(2)	PORTABLE STORAGE DEVICES — RESTRICTED USE	S
AC-20(3)	NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE	S
AC-20(4)	NETWORK ACCESSIBLE STORAGE DEVICES — PROHIBITED USE	S
AC-20(5)	PORTABLE STORAGE DEVICES — PROHIBITED USE	S
AC-21	**Information Sharing**	SP
AC-21(1)	AUTOMATED DECISION SUPPORT	S
AC-21(2)	INFORMATION SEARCH AND RETRIEVAL	S
AC-22	**Publicly Accessible Content**	SP
AC-23	**Data Mining Protection**	SP
AC-24	**Access Control Decisions**	S
AC-24(1)	TRANSMIT ACCESS AUTHORIZATION INFORMATION	S
AC-24(2)	NO USER OR PROCESS IDENTITY	S
AC-25	**Reference Monitor**	S

AWARENESS AND TRAINING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
AT-1	**Policy and Procedures**	SP
AT-2	**Literacy Training and Awareness**	SP
AT-2(1)	PRACTICAL EXERCISES	SP
AT-2(2)	INSIDER THREAT	SP
AT-2(3)	SOCIAL ENGINEERING AND MINING	SP
AT-2(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	S
AT-2(5)	ADVANCED PERSISTENT THREAT	S
AT-2(6)	CYBER THREAT ENVIRONMENT	S
AT-3	**Role-Based Training**	SP
AT-3(1)	ENVIRONMENTAL CONTROLS	S
AT-3(2)	PHYSICAL SECURITY CONTROLS	S
AT-3(3)	PRACTICAL EXERCISES	SP
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	
AT-3(5)	PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	P
AT-4	**Training Records**	SP
AT-5	**Contacts with Security Groups and Associations**	
AT-6	**Training Feedback**	SP

AUDIT AND ACCOUNTABILITY FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
AU-1	**Policy and Procedures**	SP
AU-2	**Event Logging**	S
AU-2(1)	COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES	
AU-2(2)	SELECTION OF AUDIT EVENTS BY COMPONENT	
AU-2(3)	REVIEWS AND UPDATES	
AU-2(4)	PRIVILEGED FUNCTIONS	
AU-3	**Content of Audit Records**	S
AU-3(1)	ADDITIONAL AUDIT INFORMATION	S
AU-3(2)	CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT	
AU-3(3)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	SP
AU-4	**Audit Log Storage Capacity**	S
AU-4(1)	TRANSFER TO ALTERNATE STORAGE	S
AU-5	**Response to Audit Logging Process Failures**	S
AU-5(1)	STORAGE CAPACITY WARNING	S
AU-5(2)	REAL-TIME ALERTS	S
AU-5(3)	CONFIGURABLE TRAFFIC VOLUME THRESHOLDS	S
AU-5(4)	SHUTDOWN ON FAILURE	S
AU-5(5)	ALTERNATE AUDIT LOGGING CAPABILITY	S
AU-6	**Audit Record Review, Analysis, and Reporting**	S
AU-6(1)	AUTOMATED PROCESS INTEGRATION	S
AU-6(2)	AUTOMATED SECURITY ALERTS	
AU-6(3)	CORRELATE AUDIT RECORD REPOSITORIES	S
AU-6(4)	CENTRAL REVIEW AND ANALYSIS	S
AU-6(5)	INTEGRATED ANALYSIS OF AUDIT RECORDS	S
AU-6(6)	CORRELATION WITH PHYSICAL MONITORING	S
AU-6(7)	PERMITTED ACTIONS	S
AU-6(8)	FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS	S
AU-6(9)	CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES	S
AU-6(10)	AUDIT LEVEL ADJUSTMENT	
AU-7	**Audit Record Reduction and Report Generation**	S
AU-7(1)	AUTOMATIC PROCESSING	S
AU-7(2)	AUTOMATIC SEARCH AND SORT	
AU-8	**Time Stamps**	S
AU-8(1)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	
AU-8(2)	SECONDARY AUTHORITATIVE TIME SOURCE	
AU-9	**Protection of Audit Information**	S
AU-9(1)	HARDWARE WRITE-ONCE MEDIA	S
AU-9(2)	STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS	S
AU-9(3)	CRYPTOGRAPHIC PROTECTION	S
AU-9(4)	ACCESS BY SUBSET OF PRIVILEGED USERS	S
AU-9(5)	DUAL AUTHORIZATION	S
AU-9(6)	READ-ONLY ACCESS	S

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
AU-9(7)	STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM	S
AU-10	**Non-repudiation**	S
AU-10(1)	ASSOCIATION OF IDENTITIES	S
AU-10(2)	VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY	S
AU-10(3)	CHAIN OF CUSTODY	S
AU-10(4)	VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY	S
AU-10(5)	DIGITAL SIGNATURES	
AU-11	**Audit Record Retention**	S
AU-11(1)	LONG-TERM RETRIEVAL CAPABILITY	S
AU-12	**Audit Record Generation**	S
AU-12(1)	SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL	S
AU-12(2)	STANDARDIZED FORMATS	S
AU-12(3)	CHANGES BY AUTHORIZED INDIVIDUALS	S
AU-12(4)	QUERY PARAMETER AUDITS OF PERSONALLY IDENTIFIABLE INFORMATION	S
AU-13	**Monitoring for Information Disclosure**	S
AU-13(1)	USE OF AUTOMATED TOOLS	S
AU-13(2)	REVIEW OF MONITORED SITES	S
AU-13(3)	UNAUTHORIZED REPLICATION OF INFORMATION	S
AU-14	**Session Audit**	S
AU-14(1)	SYSTEM START-UP	S
AU-14(2)	CAPTURE AND RECORD CONTENT	
AU-14(3)	REMOTE VIEWING AND LISTENING	S
AU-15	**Alternate Audit Logging Capability**	
AU-16	**Cross-Organizational Audit Logging**	S
AU-16(1)	IDENTITY PRESERVATION	S
AU-16(2)	SHARING OF AUDIT INFORMATION	S
AU-16(3)	DISASSOCIABILITY	SP

ASSESSMENT, AUTHORIZATION, AND MONITORING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
CA-1	**Policy and Procedures**	SP
CA-2	**Control Assessments**	SP
CA-2(1)	INDEPENDENT ASSESSORS	SP
CA-2(2)	SPECIALIZED ASSESSMENTS	SP
CA-2(3)	LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS	SP
CA-3	**Information Exchange**	SP
CA-3(1)	UNCLASSIFIED NATIONAL SECURITY CONNECTIONS	
CA-3(2)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	
CA-3(3)	UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS	
CA-3(4)	CONNECTIONS TO PUBLIC NETWORKS	
CA-3(5)	RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS	
CA-3(6)	TRANSFER AUTHORIZATIONS	SP
CA-3(7)	TRANSITIVE INFORMATION EXCHANGES	SP
CA-4	**Security Certification**	
CA-5	**Plan of Action and Milestones**	SP
CA-5(1)	AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY	SP
CA-6	**Authorization**	SP
CA-6(1)	JOINT AUTHORIZATION — INTRA-ORGANIZATION	SP
CA-6(2)	JOINT AUTHORIZATION — INTER-ORGANIZATION	SP
CA-7	**Continuous Monitoring**	SP
CA-7(1)	INDEPENDENT ASSESSMENT	SP
CA-7(2)	TYPES OF ASSESSMENTS	
CA-7(3)	TREND ANALYSES	SP
CA-7(4)	RISK MONITORING	SP
CA-7(5)	CONSISTENCY ANALYSIS	SP
CA-7(6)	AUTOMATION SUPPORT FOR MONITORING	SP
CA-8	**Penetration Testing**	S
CA-8(1)	INDEPENDENT PENETRATION TESTING AGENT OR TEAM	S
CA-8(2)	RED TEAM EXERCISES	S
CA-8(3)	FACILITY PENETRATION TESTING	S
CA-9	**Internal System Connections**	S
CA-9(1)	COMPLIANCE CHECKS	SP

CONFIGURATION MANAGEMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
CM-1	**Policy and Procedures**	SP
CM-2	**Baseline Configuration**	S
CM-2(1)	REVIEWS AND UPDATES	
CM-2(2)	AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY	S
CM-2(3)	RETENTION OF PREVIOUS CONFIGURATIONS	S
CM-2(4)	UNAUTHORIZED SOFTWARE	
CM-2(5)	AUTHORIZED SOFTWARE	
CM-2(6)	DEVELOPMENT AND TEST ENVIRONMENTS	S
CM-2(7)	CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS	S
CM-3	**Configuration Change Control**	SP
CM-3(1)	AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES	S
CM-3(2)	TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES	S
CM-3(3)	AUTOMATED CHANGE IMPLEMENTATION	S
CM-3(4)	SECURITY AND PRIVACY REPRESENTATIVES	SP
CM-3(5)	AUTOMATED SECURITY RESPONSE	S
CM-3(6)	CRYPTOGRAPHY MANAGEMENT	S
CM-3(7)	REVIEW SYSTEM CHANGES	S
CM-3(8)	PREVENT OR RESTRICT CONFIGURATION CHANGES	S
CM-4	**Impact Analyses**	SP
CM-4(1)	SEPARATE TEST ENVIRONMENTS	SP
CM-4(2)	VERIFICATION OF CONTROLS	SP
CM-5	**Access Restrictions for Change**	S
CM-5(1)	AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS	S
CM-5(2)	REVIEW SYSTEM CHANGES	
CM-5(3)	SIGNED COMPONENTS	
CM-5(4)	DUAL AUTHORIZATION	S
CM-5(5)	PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION	S
CM-5(6)	LIMIT LIBRARY PRIVILEGES	S
CM-5(7)	AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS	
CM-6	**Configuration Settings**	S
CM-6(1)	AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION	S
CM-6(2)	RESPOND TO UNAUTHORIZED CHANGES	S
CM-6(3)	UNAUTHORIZED CHANGE DETECTION	
CM-6(4)	CONFORMANCE DEMONSTRATION	
CM-7	**Least Functionality**	S
CM-7(1)	PERIODIC REVIEW	S
CM-7(2)	PREVENT PROGRAM EXECUTION	S
CM-7(3)	REGISTRATION COMPLIANCE	S
CM-7(4)	UNAUTHORIZED SOFTWARE	S
CM-7(5)	AUTHORIZED SOFTWARE	S
CM-7(6)	CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES	S
CM-7(7)	CODE EXECUTION IN PROTECTED ENVIRONMENTS	S

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
CM-7(8)	BINARY OR MACHINE EXECUTABLE CODE	S
CM-7(9)	PROHIBITING THE USE OF UNAUTHORIZED HARDWARE	S
CM-8	**System Component Inventory**	S
CM-8(1)	UPDATES DURING INSTALLATION AND REMOVAL	S
CM-8(2)	AUTOMATED MAINTENANCE	S
CM-8(3)	AUTOMATED UNAUTHORIZED COMPONENT DETECTION	S
CM-8(4)	ACCOUNTABILITY INFORMATION	S
CM-8(5)	NO DUPLICATE ACCOUNTING OF COMPONENTS	S
CM-8(5)	NO DUPLICATE ACCOUNTING OF COMPONENTS	
CM-8(6)	ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS	S
CM-8(7)	CENTRALIZED REPOSITORY	S
CM-8(8)	AUTOMATED LOCATION TRACKING	S
CM-8(9)	ASSIGNMENT OF COMPONENTS TO SYSTEMS	S
CM-9	**Configuration Management Plan**	S
CM-9(1)	ASSIGNMENT OF RESPONSIBILITY	S
CM-10	**Software Usage Restrictions**	S
CM-10(1)	OPEN-SOURCE SOFTWARE	S
CM-11	**User-Installed Software**	S
CM-11(1)	ALERTS FOR UNAUTHORIZED INSTALLATIONS	
CM-11(2)	SOFTWARE INSTALLATION WITH PRIVILEGED STATUS	S
CM-11(3)	AUTOMATED ENFORCEMENT AND MONITORING	S
CM-12	**Information Location**	SP
CM-12(1)	AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION	S
CM-13	**Data Action Mapping**	SP
CM-14	**Signed Components**	S

CONTINGENCY PLANNING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
CP-1	**Policy and Procedures**	SP
CP-2	**Contingency Plan**	SP
CP-2(1)	COORDINATE WITH RELATED PLANS	SP
CP-2(2)	CAPACITY PLANNING	S
CP-2(3)	RESUME MISSION AND BUSINESS FUNCTIONS	S
CP-2(4)	RESUME ALL MISSION AND BUSINESS FUNCTIONS	
CP-2(5)	CONTINUE MISSION AND BUSINESS FUNCTIONS	S
CP-2(6)	ALTERNATE PROCESSING AND STORAGE SITES	S
CP-2(7)	COORDINATE WITH EXTERNAL SERVICE PROVIDERS	SP
CP-2(8)	IDENTIFY CRITICAL ASSETS	S
CP-3	**Contingency Training**	SP
CP-3(1)	SIMULATED EVENTS	S
CP-3(2)	MECHANISMS USED IN TRAINING ENVIRONMENTS	S
CP-4	**Contingency Plan Testing**	S
CP-4(1)	COORDINATE WITH RELATED PLANS	SP
CP-4(2)	ALTERNATE PROCESSING SITE	S
CP-4(3)	AUTOMATED TESTING	S
CP-4(4)	FULL RECOVERY AND RECONSTITUTION	S
CP-4(5)	SELF-CHALLENGE	S
CP-5	**Contingency Plan Update**	S
CP-6	**Alternate Storage Site**	S
CP-6(1)	SEPARATION FROM PRIMARY SITE	S
CP-6(2)	RECOVERY TIME AND RECOVERY POINT OBJECTIVES	S
CP-6(3)	ACCESSIBILITY	S
CP-7	**Alternate Processing Site**	S
CP-7(1)	SEPARATION FROM PRIMARY SITE	S
CP-7(2)	ACCESSIBILITY	S
CP-7(3)	PRIORITY OF SERVICE	S
CP-7(4)	PREPARATION FOR USE	S
CP-7(5)	EQUIVALENT INFORMATION SECURITY SAFEGUARDS	
CP-7(6)	INABILITY TO RETURN TO PRIMARY SITE	S
CP-8	**Telecommunications Services**	S
CP-8(1)	PRIORITY OF SERVICE PROVISIONS	S
CP-8(2)	SINGLE POINTS OF FAILURE	S
CP-8(3)	SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS	S
CP-8(4)	PROVIDER CONTINGENCY PLAN	S
CP-8(5)	ALTERNATE TELECOMMUNICATION SERVICE TESTING	S
CP-9	**System Backup**	S
CP-9(1)	TESTING FOR RELIABILITY AND INTEGRITY	S
CP-9(2)	TEST RESTORATION USING SAMPLING	S
CP-9(3)	SEPARATE STORAGE FOR CRITICAL INFORMATION	S
CP-9(4)	PROTECTION FROM UNAUTHORIZED MODIFICATION	
CP-9(5)	TRANSFER TO ALTERNATE STORAGE SITE	S

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
CP-9(6)	REDUNDANT SECONDARY SYSTEM	
CP-9(7)	DUAL AUTHORIZATION	S
CP-9(8)	CRYPTOGRAPHIC PROTECTION	S
CP-10	**System Recovery and Reconstitution**	S
CP-10(1)	CONTINGENCY PLAN TESTING	
CP-10(2)	TRANSACTION RECOVERY	S
CP-10(3)	COMPENSATING SECURITY CONTROLS	
CP-10(4)	RESTORE WITHIN TIME PERIOD	S
CP-10(5)	FAILOVER CAPABILITY	
CP-10(6)	COMPONENT PROTECTION	S
CP-11	**Alternate Communications Protocols**	S
CP-12	**Safe Mode**	S
CP-13	**Alternative Security Mechanisms**	S

IDENTIFICATION AND AUTHENTICATION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
IA-1	**Policy and Procedures**	SP
IA-2	**Identification and Authentication (Organizational Users)**	SP
IA-2(1)	MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS	S
IA-2(2)	MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS	S
IA-2(3)	LOCAL ACCESS TO PRIVILEGED ACCOUNTS	
IA-2(4)	LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS	
IA-2(5)	INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION	S
IA-2(6)	ACCESS TO ACCOUNTS — SEPARATE DEVICE	S
IA-2(7)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — SEPARATE DEVICE	
IA-2(8)	ACCESS TO ACCOUNTS — REPLAY RESISTANT	S
IA-2(9)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — REPLAY RESISTANT	
IA-2(10)	SINGLE SIGN-ON	S
IA-2(11)	REMOTE ACCESS — SEPARATE DEVICE	
IA-2(12)	ACCEPTANCE OF PIV CREDENTIALS	S
IA-2(13)	OUT-OF-BAND AUTHENTICATION	S
IA-3	**Device Identification and Authentication**	S
IA-3(1)	CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION	S
IA-3(2)	CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION	
IA-3(3)	DYNAMIC ADDRESS ALLOCATION	S
IA-3(4)	DEVICE ATTESTATION	S
IA-4	**Identifier Management**	S
IA-4(1)	PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS	S
IA-4(2)	SUPERVISOR AUTHORIZATION	
IA-4(3)	MULTIPLE FORMS OF CERTIFICATION	
IA-4(4)	IDENTIFY USER STATUS	S
IA-4(5)	DYNAMIC MANAGEMENT	S
IA-4(6)	CROSS-ORGANIZATION MANAGEMENT	S
IA-4(7)	IN-PERSON REGISTRATION	
IA-4(8)	PAIRWISE PSEUDONYMOUS IDENTIFIERS	S
IA-4(9)	ATTRIBUTE MAINTENANCE AND PROTECTION	S
IA-5	**Authenticator Management**	S
IA-5(1)	PASSWORD-BASED AUTHENTICATION	S
IA-5(2)	PUBLIC KEY-BASED AUTHENTICATION	S
IA-5(3)	IN-PERSON OR TRUSTED EXTERNAL PARTY REGISTRATION	
IA-5(4)	AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION	
IA-5(5)	CHANGE AUTHENTICATORS PRIOR TO DELIVERY	S
IA-5(6)	PROTECTION OF AUTHENTICATORS	S
IA-5(7)	NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS	S
IA-5(8)	MULTIPLE SYSTEM ACCOUNTS	S
IA-5(9)	FEDERATED CREDENTIAL MANAGEMENT	S
IA-5(10)	DYNAMIC CREDENTIAL BINDING	S

CONTROL NUMBER	**CONTROL NAME** CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
IA-5(11)	HARDWARE TOKEN-BASED AUTHENTICATION	
IA-5(12)	BIOMETRIC AUTHENTICATION PERFORMANCE	S
IA-5(13)	EXPIRATION OF CACHED AUTHENTICATORS	S
IA-5(14)	MANAGING CONTENT OF PKI TRUST STORES	S
IA-5(15)	GSA-APPROVED PRODUCTS AND SERVICES	S
IA-5(16)	IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE	S
IA-5(17)	PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS	S
IA-5(18)	PASSWORD MANAGERS	S
IA-6	**Authentication Feedback**	S
IA-7	**Cryptographic Module Authentication**	S
IA-8	**Identification and Authentication (Non-Organizational Users)**	S
IA-8(1)	ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES	S
IA-8(2)	ACCEPTANCE OF EXTERNAL AUTHENTICATORS	S
IA-8(3)	USE OF FICAM-APPROVED PRODUCTS	
IA-8(4)	USE OF DEFINED PROFILES	S
IA-8(5)	ACCEPTANCE OF PIV-I CREDENTIALS	S
IA-8(6)	DISASSOCIABILITY	SP
IA-9	**Service Identification and Authentication**	S
IA-9(1)	INFORMATION EXCHANGE	
IA-9(2)	TRANSMISSION OF DECISIONS	
IA-10	**Adaptive Authentication**	S
IA-11	**Re-authentication**	S
IA-12	**Identity Proofing**	SP
IA-12(1)	SUPERVISOR AUTHORIZATION	S
IA-12(2)	IDENTITY EVIDENCE	S
IA-12(3)	IDENTITY EVIDENCE VALIDATION AND VERIFICATION	S
IA-12(4)	IN-PERSON VALIDATION AND VERIFICATION	S
IA-12(5)	ADDRESS CONFIRMATION	S
IA-12(6)	ACCEPT EXTERNALLY-PROOFED IDENTITIES	S

INCIDENT RESPONSE FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
IR-1	**Policy and Procedures**	SP
IR-2	**Incident Response Training**	SP
IR-2(1)	SIMULATED EVENTS	SP
IR-2(2)	AUTOMATED TRAINING ENVIRONMENTS	S
IR-2(3)	BREACH	P
IR-3	**Incident Response Testing**	SP
IR-3(1)	AUTOMATED TESTING	S
IR-3(2)	COORDINATION WITH RELATED PLANS	S
IR-3(3)	CONTINUOUS IMPROVEMENT	SP
IR-4	**Incident Handling**	SP
IR-4(1)	AUTOMATED INCIDENT HANDLING PROCESSES	S
IR-4(2)	DYNAMIC RECONFIGURATION	S
IR-4(3)	CONTINUITY OF OPERATIONS	S
IR-4(4)	INFORMATION CORRELATION	S
IR-4(5)	AUTOMATIC DISABLING OF SYSTEM	S
IR-4(6)	INSIDER THREATS	SP
IR-4(7)	INSIDER THREATS — INTRA-ORGANIZATION COORDINATION	SP
IR-4(8)	CORRELATION WITH EXTERNAL ORGANIZATIONS	SP
IR-4(9)	DYNAMIC RESPONSE CAPABILITY	S
IR-4(10)	SUPPLY CHAIN COORDINATION	SP
IR-4(11)	INTEGRATED INCIDENT RESPONSE TEAM	SP
IR-4(12)	MALICIOUS CODE AND FORENSIC ANALYSIS	S
IR-4(13)	BEHAVIOR ANALYSIS	S
IR-4(14)	SECURITY OPERATIONS CENTER	S
IR-4(15)	PUBLIC RELATIONS AND REPUTATION REPAIR	SP
IR-5	**Incident Monitoring**	SP
IR-5(1)	AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS	S
IR-6	**Incident Reporting**	SP
IR-6(1)	AUTOMATED REPORTING	S
IR-6(2)	VULNERABILITIES RELATED TO INCIDENTS	S
IR-6(3)	SUPPLY CHAIN COORDINATION	S
IR-7	**Incident Response Assistance**	S
IR-7(1)	AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT	S
IR-7(2)	COORDINATION WITH EXTERNAL PROVIDERS	S
IR-8	**Incident Response Plan**	SP
IR-8(1)	BREACHES	P
IR-9	**Information Spillage Response**	S
IR-9(1)	RESPONSIBLE PERSONNEL	
IR-9(2)	TRAINING	SP
IR-9(3)	POST-SPILL OPERATIONS	SP
IR-9(4)	EXPOSURE TO UNAUTHORIZED PERSONNEL	SP

MAINTENANCE FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
MA-1	**Policy and Procedures**	SP
MA-2	**Controlled Maintenance**	S
MA-2(1)	RECORD CONTENT	
MA-2(2)	AUTOMATED MAINTENANCE ACTIVITIES	S
MA-3	**Maintenance Tools**	S
MA-3(1)	INSPECT TOOLS	S
MA-3(2)	INSPECT MEDIA	S
MA-3(3)	PREVENT UNAUTHORIZED REMOVAL	S
MA-3(4)	RESTRICTED TOOL USE	S
MA-3(5)	EXECUTION WITH PRIVILEGE	S
MA-3(6)	SOFTWARE UPDATES AND PATCHES	S
MA-4	**Nonlocal Maintenance**	S
MA-4(1)	LOGGING AND REVIEW	S
MA-4(2)	DOCUMENT NONLOCAL MAINTENANCE	
MA-4(3)	COMPARABLE SECURITY AND SANITIZATION	S
MA-4(4)	AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS	S
MA-4(5)	APPROVALS AND NOTIFICATIONS	S
MA-4(6)	CRYPTOGRAPHIC PROTECTION	S
MA-4(7)	DISCONNECT VERIFICATION	S
MA-5	**Maintenance Personnel**	S
MA-5(1)	INDIVIDUALS WITHOUT APPROPRIATE ACCESS	S
MA-5(2)	SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS	S
MA-5(3)	CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS	S
MA-5(4)	FOREIGN NATIONALS	S
MA-5(5)	NON-SYSTEM MAINTENANCE	S
MA-6	**Timely Maintenance**	S
MA-6(1)	PREVENTIVE MAINTENANCE	S
MA-6(2)	PREDICTIVE MAINTENANCE	S
MA-6(3)	AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE	S
MA-7	**Field Maintenance**	S

MEDIA PROTECTION FAMILY

CONTROL NUMBER	**CONTROL NAME** CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
MP-1	**Policy and Procedures**	SP
MP-2	**Media Access**	S
MP-2(1)	AUTOMATED RESTRICTED ACCESS	
MP-2(2)	CRYPTOGRAPHIC PROTECTION	
MP-3	**Media Marking**	S
MP-4	**Media Storage**	S
MP-4(1)	CRYPTOGRAPHIC PROTECTION	
MP-4(2)	AUTOMATED RESTRICTED ACCESS	S
MP-5	**Media Transport**	S
MP-5(1)	PROTECTION OUTSIDE OF CONTROLLED AREAS	
MP-5(2)	DOCUMENTATION OF ACTIVITIES	
MP-5(3)	CUSTODIANS	S
MP-5(4)	CRYPTOGRAPHIC PROTECTION	
MP-6	**Media Sanitization**	S
MP-6(1)	REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY	S
MP-6(2)	EQUIPMENT TESTING	S
MP-6(3)	NONDESTRUCTIVE TECHNIQUES	S
MP-6(4)	CONTROLLED UNCLASSIFIED INFORMATION	
MP-6(5)	CLASSIFIED INFORMATION	
MP-6(6)	MEDIA DESTRUCTION	
MP-6(7)	DUAL AUTHORIZATION	S
MP-6(8)	REMOTE PURGING OR WIPING OF INFORMATION	S
MP-7	**Media Use**	S
MP-7(1)	PROHIBIT USE WITHOUT OWNER	
MP-7(2)	PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA	S
MP-8	**Media Downgrading**	S
MP-8(1)	DOCUMENTATION OF PROCESS	S
MP-8(2)	EQUIPMENT TESTING	S
MP-8(3)	CONTROLLED UNCLASSIFIED INFORMATION	S
MP-8(4)	CLASSIFIED INFORMATION	S

PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
PE-1	**Policy and Procedures**	SP
PE-2	**Physical Access Authorizations**	S
PE-2(1)	ACCESS BY POSITION AND ROLE	S
PE-2(2)	TWO FORMS OF IDENTIFICATION	S
PE-2(3)	RESTRICT UNESCORTED ACCESS	S
PE-3	**Physical Access Control**	S
PE-3(1)	SYSTEM ACCESS	S
PE-3(2)	FACILITY AND SYSTEMS	S
PE-3(3)	CONTINUOUS GUARDS	S
PE-3(4)	LOCKABLE CASINGS	S
PE-3(5)	TAMPER PROTECTION	S
PE-3(6)	FACILITY PENETRATION TESTING	
PE-3(7)	PHYSICAL BARRIERS	S
PE-3(8)	ACCESS CONTROL VESTIBULES	S
PE-4	**Access Control for Transmission**	S
PE-5	**Access Control for Output Devices**	S
PE-5(1)	ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS	
PE-5(2)	LINK TO INDIVIDUAL IDENTITY	S
PE-5(3)	MARKING OUTPUT DEVICES	
PE-6	**Monitoring Physical Access**	S
PE-6(1)	INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT	S
PE-6(2)	AUTOMATED INTRUSION RECOGNITION AND RESPONSES	S
PE-6(3)	VIDEO SURVEILLANCE	SP
PE-6(4)	MONITORING PHYSICAL ACCESS TO SYSTEMS	S
PE-7	**Visitor Control**	
PE-8	**Visitor Access Records**	SP
PE-8(1)	AUTOMATED RECORDS MAINTENANCE AND REVIEW	S
PE-8(2)	PHYSICAL ACCESS RECORDS	
PE-8(3)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	S
PE-9	**Power Equipment and Cabling**	S
PE-9(1)	REDUNDANT CABLING	S
PE-9(2)	AUTOMATIC VOLTAGE CONTROLS	S
PE-10	**Emergency Shutoff**	S
PE-10(1)	ACCIDENTAL AND UNAUTHORIZED ACTIVATION	
PE-11	**Emergency Power**	S
PE-11(1)	ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY	S
PE-11(2)	ALTERNATE POWER SUPPLY — SELF-CONTAINED	S
PE-12	**Emergency Lighting**	S
PE-12(1)	ESSENTIAL MISSION AND BUSINESS FUNCTIONS	S
PE-13	**Fire Protection**	S
PE-13(1)	DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION	S
PE-13(2)	SUPPRESSION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION	S
PE-13(3)	AUTOMATIC FIRE SUPPRESSION	

CONTROL NUMBER	**CONTROL NAME** CONTROL ENHANCEMENT NAME	**COLLABORATION INDEX VALUE**
PE-13(4)	INSPECTIONS	S
PE-14	**Environmental Controls**	S
PE-14(1)	AUTOMATIC CONTROLS	S
PE-14(2)	MONITORING WITH ALARMS AND NOTIFICATIONS	S
PE-15	**Water Damage Protection**	S
PE-15(1)	AUTOMATION SUPPORT	S
PE-16	**Delivery and Removal**	S
PE-17	**Alternate Work Site**	S
PE-18	**Location of System Components**	S
PE-18(1)	FACILITY SITE	
PE-19	**Information Leakage**	S
PE-19(1)	NATIONAL EMISSIONS AND TEMPEST POLICIES AND PROCEDURES	S
PE-20	**Asset Monitoring and Tracking**	S
PE-21	**Electromagnetic Pulse Protection**	S
PE-22	**Component Marking**	S
PE-23	**Facility Location**	S

PLANNING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
PL-1	**Policy and Procedures**	SP
PL-2	**System Security and Privacy Plans**	SP
PL-2(1)	CONCEPT OF OPERATIONS	
PL-2(2)	FUNCTIONAL ARCHITECTURE	
PL-2(3)	PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	
PL-3	**System Security Plan Update**	
PL-4	**Rules of Behavior**	SP
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	SP
PL-5	**Privacy Impact Assessment**	
PL-6	**Security-Related Activity Planning**	
PL-7	**Concept of Operations**	SP
PL-8	**Security and Privacy Architectures**	SP
PL-8(1)	DEFENSE IN DEPTH	S
PL-8(2)	SUPPLIER DIVERSITY	S
PL-9	**Central Management**	SP
PL-10	**Baseline Selection**	SP
PL-11	**Baseline Tailoring**	SP

PROGRAM MANAGEMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
PM-1	**Information Security Program Plan**	S
PM-2	**Information Security Program Leadership Role**	S
PM-3	**Information Security and Privacy Resources**	SP
PM-4	**Plan of Action and Milestones Process**	SP
PM-5	**System Inventory**	S
PM-5(1)	INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION	P
PM-6	**Measures of Performance**	SP
PM-7	**Enterprise Architecture**	SP
PM-7(1)	OFFLOADING	S
PM-8	**Critical Infrastructure Plan**	SP
PM-9	**Risk Management Strategy**	SP
PM-10	**Authorization Process**	SP
PM-11	**Mission and Business Process Definition**	SP
PM-12	**Insider Threat Program**	SP
PM-13	**Security and Privacy Workforce**	SP
PM-14	**Testing, Training, and Monitoring**	SP
PM-15	**Security and Privacy Groups and Associations**	SP
PM-16	**Threat Awareness Program**	S
PM-16(1)	AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE	S
PM-17	**Protecting Controlled Unclassified Information on External Systems**	SP
PM-18	**Privacy Program Plan**	P
PM-19	**Privacy Program Leadership Role**	P
PM-20	**Dissemination of Privacy Program Information**	P
PM-20(1)	PRIVACY POLICIES ON WEBSITES, APPLICATIONS, AND DIGITAL SERVICES	P
PM-21	**Accounting of Disclosures**	P
PM-22	**Personally Identifiable Information Quality Management**	P
PM-23	**Data Governance Body**	SP
PM-24	**Data Integrity Board**	P
PM-25	**Minimization of Personally Identifiable Information Used in Testing, Training, and Research**	P
PM-26	**Complaint Management**	SP
PM-27	**Privacy Reporting**	P
PM-28	**Risk Framing**	SP
PM-29	**Risk Management Program Leadership Roles**	SP
PM-30	**Supply Chain Risk Management Strategy**	S
PM-30(1)	SUPPLIERS OF CRITICAL OR MISSION-ESSENTIAL ITEMS	S
PM-31	**Continuous Monitoring Strategy**	SP
PM-32	**Purposing**	S

PERSONNEL SECURITY FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
PS-1	**Policy and Procedures**	SP
PS-2	**Position Risk Designation**	S
PS-3	**Personnel Screening**	S
PS-3(1)	CLASSIFIED INFORMATION	S
PS-3(2)	FORMAL INDOCTRINATION	S
PS-3(3)	INFORMATION WITH SPECIAL PROTECTION MEASURES	S
PS-3(4)	CITIZENSHIP REQUIREMENTS	S
PS-4	**Personnel Termination**	S
PS-4(1)	POST-EMPLOYMENT REQUIREMENTS	S
PS-4(2)	AUTOMATED ACTIONS	S
PS-5	**Personnel Transfer**	S
PS-6	**Access Agreements**	S
PS-6(1)	INFORMATION REQUIRING SPECIAL PROTECTION	
PS-6(2)	CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION	S
PS-6(3)	POST-EMPLOYMENT REQUIREMENTS	S
PS-7	**External Personnel Security**	S
PS-8	**Personnel Sanctions**	SP
PS-9	**Position Descriptions**	SP

PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
PT-1	**Policy and Procedures**	P
PT-2	**Authority to Process Personally Identifiable Information**	P
PT-2(1)	DATA TAGGING	SP
PT-2(2)	AUTOMATION	S
PT-3	**Personally Identifiable Information Processing Purposes**	P
PT-3(1)	DATA TAGGING	SP
PT-3(2)	AUTOMATION	S
PT-4	**Consent**	P
PT-4(1)	TAILORED CONSENT	P
PT-4(2)	JUST-IN-TIME CONSENT	P
PT-4(3)	REVOCATION	P
PT-5	**Privacy Notice**	P
PT-5(1)	JUST-IN-TIME NOTICE	P
PT-5(2)	PRIVACY ACT STATEMENTS	P
PT-6	**System of Records Notice**	P
PT-6(1)	ROUTINE USES	P
PT-6(2)	EXEMPTION RULES	P
PT-7	**Specific Categories of Personally Identifiable Information**	P
PT-7(1)	SOCIAL SECURITY NUMBERS	P
PT-7(2)	FIRST AMENDMENT INFORMATION	P
PT-8	**Computer Matching Requirements**	P

RISK ASSESSMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
RA-1	**Policy and Procedures**	SP
RA-2	**Security Categorization**	SP
RA-2(1)	IMPACT-LEVEL PRIORITIZATION	S
RA-3	**Risk Assessment**	SP
RA-3(1)	SUPPLY CHAIN RISK ASSESSMENT	S
RA-3(2)	USE OF ALL-SOURCE INTELLIGENCE	S
RA-3(3)	DYNAMIC THREAT AWARENESS	S
RA-3(4)	PREDICTIVE CYBER ANALYTICS	S
RA-4	**Risk Assessment Update**	
RA-5	**Vulnerability Monitoring and Scanning**	S
RA-5(1)	UPDATE TOOL CAPABILITY	
RA-5(2)	UPDATE VULNERABILITIES TO BE SCANNED	S
RA-5(3)	BREADTH AND DEPTH OF COVERAGE	S
RA-5(4)	DISCOVERABLE INFORMATION	S
RA-5(5)	PRIVILEGED ACCESS	S
RA-5(6)	AUTOMATED TREND ANALYSES	S
RA-5(7)	AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS	
RA-5(8)	REVIEW HISTORIC AUDIT LOGS	S
RA-5(9)	PENETRATION TESTING AND ANALYSES	
RA-5(10)	CORRELATE SCANNING INFORMATION	S
RA-5(11)	PUBLIC DISCLOSURE PROGRAM	S
RA-6	**Technical Surveillance Countermeasures Survey**	S
RA-7	**Risk Response**	SP
RA-8	**Privacy Impact Assessments**	P
RA-9	**Criticality Analysis**	S
RA-10	**Threat Hunting**	S

SYSTEM AND SERVICES ACQUISITION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
SA-1	**Policy and Procedures**	SP
SA-2	**Allocation of Resources**	SP
SA-3	**System Development Life Cycle**	SP
SA-3(1)	MANAGE PREPRODUCTION ENVIRONMENT	S
SA-3(2)	USE OF LIVE OR OPERATIONAL DATA	SP
SA-3(3)	TECHNOLOGY REFRESH	S
SA-4	**Acquisition Process**	SP
SA-4(1)	FUNCTIONAL PROPERTIES OF CONTROLS	S
SA-4(2)	DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS	S
SA-4(3)	DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES	S
SA-4(4)	ASSIGNMENT OF COMPONENTS TO SYSTEMS	
SA-4(5)	SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS	S
SA-4(6)	USE OF INFORMATION ASSURANCE PRODUCTS	S
SA-4(7)	NIAP-APPROVED PROTECTION PROFILES	S
SA-4(8)	CONTINUOUS MONITORING PLAN FOR CONTROLS	S
SA-4(9)	FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE	S
SA-4(10)	USE OF APPROVED PIV PRODUCTS	S
SA-4(11)	SYSTEM OF RECORDS	P
SA-4(12)	DATA OWNERSHIP	S
SA-5	**System Documentation**	SP
SA-5(1)	FUNCTIONAL PROPERTIES OF SECURITY CONTROLS	
SA-5(2)	SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES	
SA-5(3)	HIGH-LEVEL DESIGN	
SA-5(4)	LOW-LEVEL DESIGN	
SA-5(5)	SOURCE CODE	
SA-6	**Software Usage Restrictions**	
SA-7	**User-Installed Software**	
SA-8	**Security and Privacy Engineering Principles**	SP
SA-8(1)	CLEAR ABSTRACTIONS	S
SA-8(2)	LEAST COMMON MECHANISM	S
SA-8(3)	MODULARITY AND LAYERING	S
SA-8(4)	PARTIALLY ORDERED DEPENDENCIES	S
SA-8(5)	EFFICIENTLY MEDIATED ACCESS	S
SA-8(6)	MINIMIZED SHARING	S
SA-8(7)	REDUCED COMPLEXITY	S
SA-8(8)	SECURE EVOLVABILITY	S
SA-8(9)	TRUSTED COMPONENTS	S
SA-8(10)	HIERARCHICAL TRUST	S
SA-8(11)	INVERSE MODIFICATION THRESHOLD	S
SA-8(12)	HIERARCHICAL PROTECTION	S
SA-8(13)	MINIMIZED SECURITY ELEMENTS	S
SA-8(14)	LEAST PRIVILEGE	S

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
SA-8(15)	PREDICATE PERMISSION	S
SA-8(16)	SELF-RELIANT TRUSTWORTHINESS	S
SA-8(17)	SECURE DISTRIBUTED COMPOSITION	S
SA-8(18)	TRUSTED COMMUNICATIONS CHANNELS	S
SA-8(19)	CONTINUOUS PROTECTION	S
SA-8(20)	SECURE METADATA MANAGEMENT	S
SA-8(21)	SELF-ANALYSIS	S
SA-8(22)	ACCOUNTABILITY AND TRACEABILITY	S
SA-8(23)	SECURE DEFAULTS	S
SA-8(24)	SECURE FAILURE AND RECOVERY	S
SA-8(25)	ECONOMIC SECURITY	S
SA-8(26)	PERFORMANCE SECURITY	S
SA-8(27)	HUMAN FACTORED SECURITY	S
SA-8(28)	ACCEPTABLE SECURITY	SP
SA-8(29)	REPEATABLE AND DOCUMENTED PROCEDURES	S
SA-8(30)	PROCEDURAL RIGOR	S
SA-8(31)	SECURE SYSTEM MODIFICATION	S
SA-8(32)	SUFFICIENT DOCUMENTATION	S
SA-8(33)	MINIMIZATION	P
SA-9	**External System Services**	S
SA-9(1)	RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS	S
SA-9(2)	IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES	S
SA-9(3)	ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS	S
SA-9(4)	CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS	S
SA-9(5)	PROCESSING, STORAGE, AND SERVICE LOCATION	S
SA-9(6)	ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS	S
SA-9(7)	ORGANIZATION-CONTROLLED INTEGRITY CHECKING	S
SA-9(8)	PROCESSING AND STORAGE LOCATION — U.S. JURISDICTION	S
SA-10	**Developer Configuration Management**	S
SA-10(1)	SOFTWARE AND FIRMWARE INTEGRITY VERIFICATION	S
SA-10(2)	ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES	S
SA-10(3)	HARDWARE INTEGRITY VERIFICATION	S
SA-10(4)	TRUSTED GENERATION	S
SA-10(5)	MAPPING INTEGRITY FOR VERSION CONTROL	S
SA-10(6)	TRUSTED DISTRIBUTION	S
SA-10(7)	SECURITY AND PRIVACY REPRESENTATIVES	S
SA-11	**Developer Testing and Evaluation**	SP
SA-11(1)	STATIC CODE ANALYSIS	S
SA-11(2)	THREAT MODELING AND VULNERABILITY ANALYSES	S
SA-11(3)	INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE	SP
SA-11(4)	MANUAL CODE REVIEWS	S
SA-11(5)	PENETRATION TESTING	S
SA-11(6)	ATTACK SURFACE REVIEWS	S
SA-11(7)	VERIFY SCOPE OF TESTING AND EVALUATION	S

CONTROL NUMBER	**CONTROL NAME** CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
SA-11(8)	DYNAMIC CODE ANALYSIS	S
SA-11(9)	INTERACTIVE APPLICATION SECURITY TESTING	S
SA-12	**Supply Chain Protection**	
SA-12(1)	ACQUISITION STRATEGIES, TOOLS, AND METHODS	
SA-12(2)	SUPPLIER REVIEWS	
SA-12(3)	TRUSTED SHIPPING AND WAREHOUSING	
SA-12(4)	DIVERSITY OF SUPPLIERS	
SA-12(5)	LIMITATION OF HARM	
SA-12(6)	MINIMIZING PROCUREMENT TIME	
SA-12(7)	ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE	
SA-12(8)	USE OF ALL-SOURCE INTELLIGENCE	
SA-12(9)	OPERATIONS SECURITY	
SA-12(10)	VALIDATE AS GENUINE AND NOT ALTERED	
SA-12(11)	PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS	
SA-12(12)	INTER-ORGANIZATIONAL AGREEMENTS	
SA-12(13)	CRITICAL INFORMATION SYSTEM COMPONENTS	
SA-12(14)	IDENTITY AND TRACEABILITY	
SA-12(15)	PROCESS TO ADDRESS WEAKNESSES OR DEFICIENCIES	
SA-13	**Trustworthiness**	
SA-14	**Criticality Analysis**	
SA-14(1)	CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING	
SA-15	**Development Process, Standards, and Tools**	SP
SA-15(1)	QUALITY METRICS	S
SA-15(2)	SECURITY AND PRIVACY TRACKING TOOLS	SP
SA-15(3)	CRITICALITY ANALYSIS	S
SA-15(4)	THREAT MODELING AND VULNERABILITY ANALYSIS	
SA-15(5)	ATTACK SURFACE REDUCTION	S
SA-15(6)	CONTINUOUS IMPROVEMENT	S
SA-15(7)	AUTOMATED VULNERABILITY ANALYSIS	S
SA-15(8)	REUSE OF THREAT AND VULNERABILITY INFORMATION	S
SA-15(9)	USE OF LIVE DATA	
SA-15(10)	INCIDENT RESPONSE PLAN	SP
SA-15(11)	ARCHIVE SYSTEM OR COMPONENT	S
SA-15(12)	MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION	P
SA-16	**Developer-Provided Training**	SP
SA-17	**Developer Security and Privacy Architecture and Design**	SP
SA-17(1)	FORMAL POLICY MODEL	SP
SA-17(2)	SECURITY-RELEVANT COMPONENTS	SP
SA-17(3)	FORMAL CORRESPONDENCE	S
SA-17(4)	INFORMAL CORRESPONDENCE	S
SA-17(5)	CONCEPTUALLY SIMPLE DESIGN	S
SA-17(6)	STRUCTURE FOR TESTING	S
SA-17(7)	STRUCTURE FOR LEAST PRIVILEGE	S
SA-17(8)	ORCHESTRATION	S

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
SA-17(9)	DESIGN DIVERSITY	S
SA-18	Tamper Resistance and Detection	
SA-18(1)	MULTIPLE PHASES OF SYSTEM DEVELOPMENT LIFE CYCLE	
SA-18(2)	INSPECTION OF SYSTEMS OR COMPONENTS	
SA-19	Component Authenticity	
SA-19(1)	ANTI-COUNTERFEIT TRAINING	
SA-19(2)	CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR	
SA-19(3)	COMPONENT DISPOSAL	
SA-19(4)	ANTI-COUNTERFEIT SCANNING	
SA-20	**Customized Development of Critical Components**	S
SA-21	**Developer Screening**	S
SA-21(1)	VALIDATION OF SCREENING	
SA-22	**Unsupported System Components**	S
SA-22(1)	ALTERNATIVE SOURCES FOR CONTINUED SUPPORT	
SA-23	**Specialization**	S

SYSTEM AND COMMUNICATIONS PROTECTION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
SC-1	**Policy and Procedures**	SP
SC-2	**Separation of System and User Functionality**	S
SC-2(1)	INTERFACES FOR NON-PRIVILEGED USERS	S
SC-2(2)	DISASSOCIABILITY	S
SC-3	**Security Function Isolation**	S
SC-3(1)	HARDWARE SEPARATION	S
SC-3(2)	ACCESS AND FLOW CONTROL FUNCTIONS	S
SC-3(3)	MINIMIZE NONSECURITY FUNCTIONALITY	S
SC-3(4)	MODULE COUPLING AND COHESIVENESS	S
SC-3(5)	LAYERED STRUCTURES	S
SC-4	**Information in Shared System Resources**	S
SC-4(1)	SECURITY LEVELS	
SC-4(2)	MULTILEVEL OR PERIODS PROCESSING	S
SC-5	**Denial-of-Service Protection**	S
SC-5(1)	RESTRICT ABILITY TO ATTACK OTHER SYSTEMS	S
SC-5(2)	CAPACITY, BANDWIDTH, AND REDUNDANCY	S
SC-5(3)	DETECTION AND MONITORING	S
SC-6	**Resource Availability**	S
SC-7	**Boundary Protection**	S
SC-7(1)	PHYSICALLY SEPARATED SUBNETWORKS	
SC-7(2)	PUBLIC ACCESS	
SC-7(3)	ACCESS POINTS	S
SC-7(4)	EXTERNAL TELECOMMUNICATIONS SERVICES	S
SC-7(5)	DENY BY DEFAULT — ALLOW BY EXCEPTION	S
SC-7(6)	RESPONSE TO RECOGNIZED FAILURES	
SC-7(7)	SPLIT TUNNELING FOR REMOTE DEVICES	S
SC-7(8)	ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS	S
SC-7(9)	RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC	S
SC-7(10)	PREVENT EXFILTRATION	S
SC-7(11)	RESTRICT INCOMING COMMUNICATIONS TRAFFIC	S
SC-7(12)	HOST-BASED PROTECTION	S
SC-7(13)	ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS	S
SC-7(14)	PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS	S
SC-7(15)	NETWORKED PRIVILEGED ACCESSES	S
SC-7(16)	PREVENT DISCOVERY OF SYSTEM COMPONENTS	S
SC-7(17)	AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS	S
SC-7(18)	FAIL SECURE	S
SC-7(19)	BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS	S
SC-7(20)	DYNAMIC ISOLATION AND SEGREGATION	S
SC-7(21)	ISOLATION OF SYSTEM COMPONENTS	S

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
SC-7(22)	SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS	S
SC-7(23)	DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE	S
SC-7(24)	PERSONALLY IDENTIFIABLE INFORMATION	SP
SC-7(25)	UNCLASSIFIED NATIONAL SECURITY CONNECTIONS	S
SC-7(26)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	S
SC-7(27)	UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS	S
SC-7(28)	CONNECTIONS TO PUBLIC NETWORKS	S
SC-7(29)	SEPARATE SUBNETS TO ISOLATE FUNCTIONS	S
SC-8	**Transmission Confidentiality and Integrity**	S
SC-8(1)	CRYPTOGRAPHIC PROTECTION	S
SC-8(2)	PRE- AND POST-TRANSMISSION HANDLING	S
SC-8(3)	CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS	S
SC-8(4)	CONCEAL OR RANDOMIZE COMMUNICATIONS	S
SC-8(5)	PROTECTED DISTRIBUTION SYSTEM	S
SC-9	**Transmission Confidentiality**	
SC-10	**Network Disconnect**	S
SC-11	**Trusted Path**	S
SC-11(1)	IRREFUTABLE COMMUNICATIONS PATH	S
SC-12	**Cryptographic Key Establishment and Management**	S
SC-12(1)	AVAILABILITY	S
SC-12(2)	SYMMETRIC KEYS	S
SC-12(3)	ASYMMETRIC KEYS	S
SC-12(4)	PKI CERTIFICATES	
SC-12(5)	PKI CERTIFICATES / HARDWARE TOKENS	
SC-12(6)	PHYSICAL CONTROL OF KEYS	S
SC-13	**Cryptographic Protection**	S
SC-13(1)	FIPS-VALIDATED CRYPTOGRAPHY	
SC-13(2)	NSA-APPROVED CRYPTOGRAPHY	
SC-13(3)	INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS	
SC-13(4)	DIGITAL SIGNATURES	
SC-14	**Public Access Protections**	
SC-15	**Collaborative Computing Devices and Applications**	S
SC-15(1)	PHYSICAL OR LOGICAL DISCONNECT	S
SC-15(2)	BLOCKING INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	
SC-15(3)	DISABLING AND REMOVAL IN SECURE WORK AREAS	S
SC-15(4)	EXPLICITLY INDICATE CURRENT PARTICIPANTS	S
SC-16	**Transmission of Security and Privacy Attributes**	SP
SC-16(1)	INTEGRITY VERIFICATION	S
SC-16(2)	ANTI-SPOOFING MECHANISMS	S
SC-16(3)	CRYPTOGRAPHIC BINDING	S
SC-17	**Public Key Infrastructure Certificates**	S
SC-18	**Mobile Code**	S
SC-18(1)	IDENTIFY UNACCEPTABLE CODE AND TAKE CORRECTIVE ACTIONS	S
SC-18(2)	ACQUISITION, DEVELOPMENT, AND USE	S

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
SC-18(3)	PREVENT DOWNLOADING AND EXECUTION	S
SC-18(4)	PREVENT AUTOMATIC EXECUTION	S
SC-18(5)	ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS	S
SC-19	Voice over Internet Protocol	
SC-20	**Secure Name/Address Resolution Service (Authoritative Source)**	S
SC-20(1)	CHILD SUBSPACES	
SC-20(2)	DATA ORIGIN AND INTEGRITY	S
SC-21	**Secure Name/Address Resolution Service (Recursive or Caching Resolver)**	S
SC-21(1)	DATA ORIGIN AND INTEGRITY	
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**	S
SC-23	**Session Authenticity**	S
SC-23(1)	INVALIDATE SESSION IDENTIFIERS AT LOGOUT	S
SC-23(2)	USER-INITIATED LOGOUTS AND MESSAGE DISPLAYS	
SC-23(3)	UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS	S
SC-23(4)	UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION	
SC-23(5)	ALLOWED CERTIFICATE AUTHORITIES	S
SC-24	**Fail in Known State**	S
SC-25	**Thin Nodes**	S
SC-26	**Decoys**	S
SC-26(1)	DETECTION OF MALICIOUS CODE	
SC-27	**Platform-Independent Applications**	S
SC-28	**Protection of Information at Rest**	SP
SC-28(1)	CRYPTOGRAPHIC PROTECTION	S
SC-28(2)	OFFLINE STORAGE	SP
SC-28(3)	CRYPTOGRAPHIC KEYS	S
SC-29	**Heterogeneity**	S
SC-29(1)	VIRTUALIZATION TECHNIQUES	S
SC-30	**Concealment and Misdirection**	S
SC-30(1)	VIRTUALIZATION TECHNIQUES	
SC-30(2)	RANDOMNESS	S
SC-30(3)	CHANGE PROCESSING AND STORAGE LOCATIONS	S
SC-30(4)	MISLEADING INFORMATION	S
SC-30(5)	CONCEALMENT OF SYSTEM COMPONENTS	S
SC-31	**Covert Channel Analysis**	S
SC-31(1)	TEST COVERT CHANNELS FOR EXPLOITABILITY	S
SC-31(2)	MAXIMUM BANDWIDTH	S
SC-31(3)	MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS	S
SC-32	**System Partitioning**	S
SC-32(1)	SEPARATE PHYSICAL DOMAINS FOR PRIVILEGED FUNCTIONS	S
SC-33	Transmission Preparation Integrity	
SC-34	**Non-Modifiable Executable Programs**	S

CONTROL NUMBER	**CONTROL NAME** CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
SC-34(1)	NO WRITABLE STORAGE	S
SC-34(2)	INTEGRITY PROTECTION AND READ-ONLY MEDIA	S
SC-34(3)	HARDWARE-BASED PROTECTION	
SC-35	**External Malicious Code Identification**	S
SC-36	**Distributed Processing and Storage**	S
SC-36(1)	POLLING TECHNIQUES	S
SC-36(2)	SYNCHRONIZATION	S
SC-37	**Out-of-Band Channels**	S
SC-37(1)	ENSURE DELIVERY AND TRANSMISSION	S
SC-38	**Operations Security**	S
SC-39	**Process Isolation**	S
SC-39(1)	HARDWARE SEPARATION	S
SC-39(2)	SEPARATE EXECUTION DOMAIN PER THREAD	S
SC-40	**Wireless Link Protection**	S
SC-40(1)	ELECTROMAGNETIC INTERFERENCE	S
SC-40(2)	REDUCE DETECTION POTENTIAL	S
SC-40(3)	IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION	S
SC-40(4)	SIGNAL PARAMETER IDENTIFICATION	S
SC-41	**Port and I/O Device Access**	S
SC-42	**Sensor Capability and Data**	S
SC-42(1)	REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES	S
SC-42(2)	AUTHORIZED USE	S
SC-42(3)	PROHIBIT USE OF DEVICES	
SC-42(4)	NOTICE OF COLLECTION	P
SC-42(5)	COLLECTION MINIMIZATION	P
SC-43	**Usage Restrictions**	S
SC-44	**Detonation Chambers**	S
SC-45	**System Time Synchronization**	S
SC-45(1)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	S
SC-45(2)	SECONDARY AUTHORITATIVE TIME SOURCE	S
SC-46	**Cross Domain Policy Enforcement**	S
SC-47	**Alternate Communications Paths**	S
SC-48	**Sensor Relocation**	S
SC-48(1)	DYNAMIC RELOCATION OF SENSORS OR MONITORING CAPABILITIES	S
SC-49	**Hardware-Enforced Separation and Policy Enforcement**	S
SC-50	**Software-Enforced Separation and Policy Enforcement**	S
SC-51	**Hardware-Based Protection**	S

SYSTEM AND INFORMATION INTEGRITY FAMILY

CONTROL NUMBER	**CONTROL NAME** CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
SI-1	**Policy and Procedures**	SP
SI-2	**Flaw Remediation**	S
SI-2(1)	CENTRAL MANAGEMENT	
SI-2(2)	AUTOMATED FLAW REMEDIATION STATUS	S
SI-2(3)	TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS	S
SI-2(4)	AUTOMATED PATCH MANAGEMENT TOOLS	S
SI-2(5)	AUTOMATIC SOFTWARE AND FIRMWARE UPDATES	S
SI-2(6)	REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE AND FIRMWARE	S
SI-3	**Malicious Code Protection**	S
SI-3(1)	CENTRAL MANAGEMENT	
SI-3(2)	AUTOMATIC UPDATES	
SI-3(3)	NON-PRIVILEGED USERS	
SI-3(4)	UPDATES ONLY BY PRIVILEGED USERS	S
SI-3(5)	PORTABLE STORAGE DEVICES	
SI-3(6)	TESTING AND VERIFICATION	S
SI-3(7)	NONSIGNATURE-BASED DETECTION	
SI-3(8)	DETECT UNAUTHORIZED COMMANDS	S
SI-3(9)	AUTHENTICATE REMOTE COMMANDS	
SI-3(10)	MALICIOUS CODE ANALYSIS	S
SI-4	**System Monitoring**	S
SI-4(1)	SYSTEM-WIDE INTRUSION DETECTION SYSTEM	S
SI-4(2)	AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS	S
SI-4(3)	AUTOMATED TOOL AND MECHANISM INTEGRATION	S
SI-4(4)	INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	S
SI-4(5)	SYSTEM-GENERATED ALERTS	S
SI-4(6)	RESTRICT NON-PRIVILEGED USERS	
SI-4(7)	AUTOMATED RESPONSE TO SUSPICIOUS EVENTS	S
SI-4(8)	PROTECTION OF MONITORING INFORMATION	
SI-4(9)	TESTING OF MONITORING TOOLS AND MECHANISMS	S
SI-4(10)	VISIBILITY OF ENCRYPTED COMMUNICATIONS	SP
SI-4(11)	ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES	S
SI-4(12)	AUTOMATED ORGANIZATION-GENERATED ALERTS	S
SI-4(13)	ANALYZE TRAFFIC AND EVENT PATTERNS	S
SI-4(14)	WIRELESS INTRUSION DETECTION	S
SI-4(15)	WIRELESS TO WIRELINE COMMUNICATIONS	S
SI-4(16)	CORRELATE MONITORING INFORMATION	S
SI-4(17)	INTEGRATED SITUATIONAL AWARENESS	S
SI-4(18)	ANALYZE TRAFFIC AND COVERT EXFILTRATION	S
SI-4(19)	RISK FOR INDIVIDUALS	SP
SI-4(20)	PRIVILEGED USERS	SP
SI-4(21)	PROBATIONARY PERIODS	SP
SI-4(22)	UNAUTHORIZED NETWORK SERVICES	S

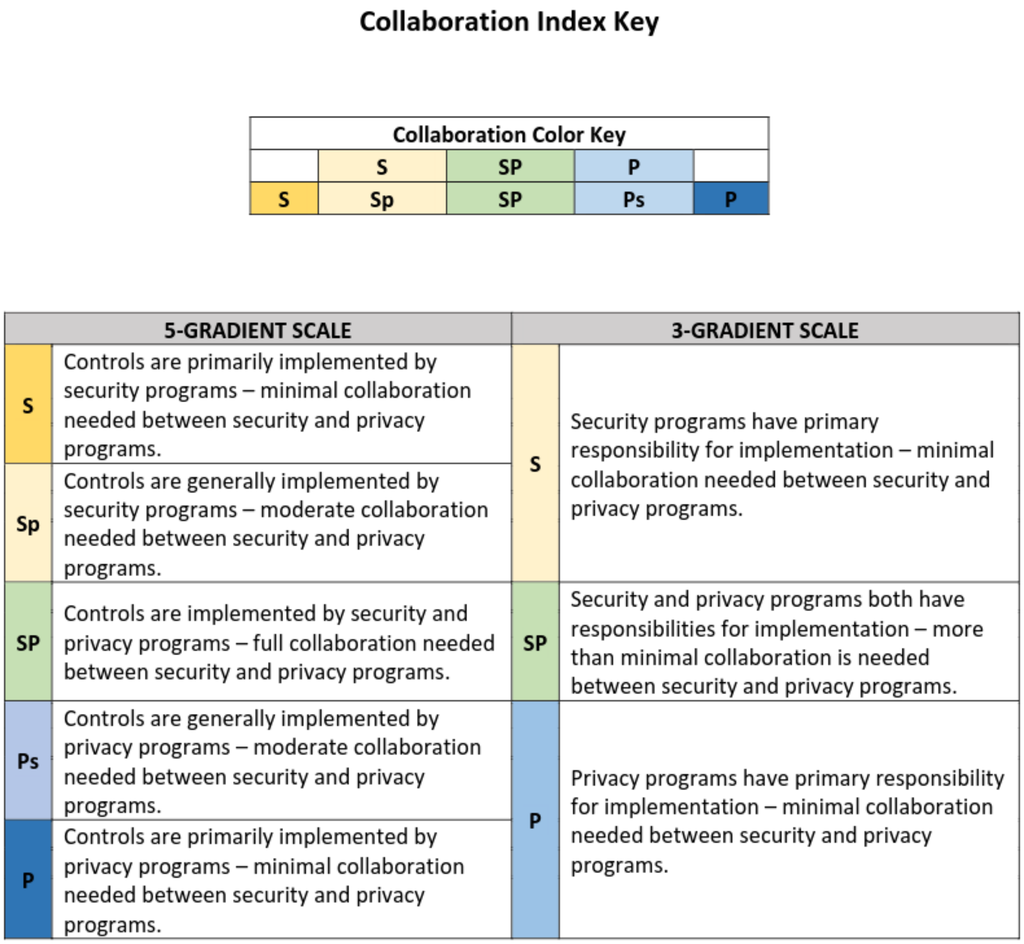
CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
SI-4(23)	HOST-BASED DEVICES	S
SI-4(24)	INDICATORS OF COMPROMISE	S
SI-4(25)	OPTIMIZE NETWORK TRAFFIC ANALYSIS	S
SI-5	**Security Alerts, Advisories, and Directives**	S
SI-5(1)	AUTOMATED ALERTS AND ADVISORIES	S
SI-6	**Security and Privacy Function Verification**	SP
SI-6(1)	NOTIFICATION OF FAILED SECURITY TESTS	
SI-6(2)	AUTOMATION SUPPORT FOR DISTRIBUTED TESTING	SP
SI-6(3)	REPORT VERIFICATION RESULTS	SP
SI-7	**Software, Firmware, and Information Integrity**	S
SI-7(1)	INTEGRITY CHECKS	S
SI-7(2)	AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS	S
SI-7(3)	CENTRALLY MANAGED INTEGRITY TOOLS	S
SI-7(4)	TAMPER-EVIDENT PACKAGING	
SI-7(5)	AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS	S
SI-7(6)	CRYPTOGRAPHIC PROTECTION	S
SI-7(7)	INTEGRATION OF DETECTION AND RESPONSE	S
SI-7(8)	AUDITING CAPABILITY FOR SIGNIFICANT EVENTS	S
SI-7(9)	VERIFY BOOT PROCESS	S
SI-7(10)	PROTECTION OF BOOT FIRMWARE	S
SI-7(11)	CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES	
SI-7(12)	INTEGRITY VERIFICATION	S
SI-7(13)	CODE EXECUTION IN PROTECTED ENVIRONMENTS	
SI-7(14)	BINARY OR MACHINE EXECUTABLE CODE	
SI-7(15)	CODE AUTHENTICATION	S
SI-7(16)	TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION	S
SI-7(17)	RUNTIME APPLICATION SELF-PROTECTION	S
SI-8	**Spam Protection**	S
SI-8(1)	CENTRAL MANAGEMENT	
SI-8(2)	AUTOMATIC UPDATES	S
SI-8(3)	CONTINUOUS LEARNING CAPABILITY	S
SI-9	**Information Input Restrictions**	
SI-10	**Information Input Validation**	S
SI-10(1)	MANUAL OVERRIDE CAPABILITY	S
SI-10(2)	REVIEW AND RESOLVE ERRORS	S
SI-10(3)	PREDICTABLE BEHAVIOR	S
SI-10(4)	TIMING INTERACTIONS	S
SI-10(5)	RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS	S
SI-10(6)	INJECTION PREVENTION	S
SI-11	**Error Handling**	S
SI-12	**Information Management and Retention**	SP
SI-12(1)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	SP
SI-12(2)	MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH	SP

CONTROL NUMBER	**CONTROL NAME** CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
SI-12(3)	INFORMATION DISPOSAL	SP
SI-13	**Predictable Failure Prevention**	S
SI-13(1)	TRANSFERRING COMPONENT RESPONSIBILITIES	S
SI-13(2)	TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION	
SI-13(3)	MANUAL TRANSFER BETWEEN COMPONENTS	S
SI-13(4)	STANDBY COMPONENT INSTALLATION AND NOTIFICATION	S
SI-13(5)	FAILOVER CAPABILITY	S
SI-14	**Non-Persistence**	S
SI-14(1)	REFRESH FROM TRUSTED SOURCES	S
SI-14(2)	NON-PERSISTENT INFORMATION	S
SI-14(3)	NON-PERSISTENT CONNECTIVITY	S
SI-15	**Information Output Filtering**	S
SI-16	**Memory Protection**	S
SI-17	**Fail-Safe Procedures**	S
SI-18	**Personally Identifiable Information Quality Operations**	P
SI-18(1)	AUTOMATION SUPPORT	SP
SI-18(2)	DATA TAGS	P
SI-18(3)	COLLECTION	P
SI-18(4)	INDIVIDUAL REQUESTS	P
SI-18(5)	NOTICE OF CORRECTION OR DELETION	P
SI-19	**De-Identification**	P
SI-19(1)	COLLECTION	P
SI-19(2)	ARCHIVING	SP
SI-19(3)	RELEASE	P
SI-19(4)	REMOVAL, MASKING, ENCRYPTION, HASHING, OR REPLACEMENT OF DIRECT IDENTIFIERS	SP
SI-19(5)	STATISTICAL DISCLOSURE CONTROL	P
SI-19(6)	DIFFERENTIAL PRIVACY	P
SI-19(7)	VALIDATED ALGORITHMS SOFTWARE	SP
SI-19(8)	MOTIVATED INTRUDER	SP
SI-20	**Tainting**	S
SI-21	**Information Refresh**	S
SI-22	**Information Diversity**	S
SI-23	**Information Fragmentation**	S

SUPPLY CHAIN RISK MANAGEMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	COLLABORATION INDEX VALUE
SR-1	**Policy and Procedures**	SP
SR-2	**Supply Chain Risk Management Plan**	SP
SR-2(1)	ESTABLISH SCRM TEAM	SP
SR-3	**Supply Chain Controls and Processes**	S
SR-3(1)	DIVERSE SUPPLY BASE	S
SR-3(2)	LIMITATION OF HARM	S
SR-3(3)	SUB-TIER FLOW DOWN	S
SR-4	**Provenance**	S
SR-4(1)	IDENTITY	S
SR-4(2)	TRACK AND TRACE	S
SR-4(3)	VALIDATE AS GENUINE AND NOT ALTERED	S
SR-4(4)	SUPPLY CHAIN INTEGRITY — PEDIGREE	S
SR-5	**Acquisition Strategies, Tools, and Methods**	S
SR-5(1)	ADEQUATE SUPPLY	S
SR-5(2)	ASSESSMENTS PRIOR TO SELECTION, ACCEPTANCE, MODIFICATION, OR UPDATE	S
SR-6	**Supplier Assessments and Reviews**	S
SR-6(1)	TESTING AND ANALYSIS	S
SR-7	**Supply Chain Operations Security**	S
SR-8	**Notification Agreements**	SP
SR-9	**Tamper Resistance and Detection**	S
SR-9(1)	MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE	S
SR-10	**Inspection of Systems or Components**	S
SR-11	**Component Authenticity**	S
SR-11(1)	ANTI-COUNTERFEIT TRAINING	S
SR-11(2)	CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR	S
SR-11(3)	ANTI-COUNTERFEIT SCANNING	S
SR-12	**Component Disposal**	S

COLLABORATION INDEX KEY



Collaboration Index Key

Collaboration Color Key				
	S	SP	P	
S	Sp	SP	Ps	P

5-GRADIENT SCALE		3-GRADIENT SCALE	
S	Controls are primarily implemented by security programs – minimal collaboration needed between security and privacy programs.	S	Security programs have primary responsibility for implementation – minimal collaboration needed between security and privacy programs.
Sp	Controls are generally implemented by security programs – moderate collaboration needed between security and privacy programs.		
SP	Controls are implemented by security and privacy programs – full collaboration needed between security and privacy programs.	SP	Security and privacy programs both have responsibilities for implementation – more than minimal collaboration is needed between security and privacy programs.
Ps	Controls are generally implemented by privacy programs – moderate collaboration needed between security and privacy programs.	P	Privacy programs have primary responsibility for implementation – minimal collaboration needed between security and privacy programs.
P	Controls are primarily implemented by privacy programs – minimal collaboration needed between security and privacy programs.		

This publication provides Collaboration Index values for each of the controls and control enhancements in NIST SP 800-53 Rev. 5. The values are provided using two different scales – a 5-gradient scale and a 3-gradient scale. The two scales were created by OMB and NIST during the development of a preliminary draft of NIST SP 800-53 Rev. 5. The only difference between the two scales is the level of resolution and granularity provided. The 5-gradient scale provides additional resolution and granularity, compared to the 3-gradient scale. The values for the 3-gradient scale are derivative of the values selected for the 5-gradient scale. For example, if an "Sp" value was selected for a particular control on the 5-gradient scale, then the selection of an "S" value was required on the 3-gradient scale.

In addition to the Collaboration Index values, this publication also uses a scheme of color coding to serve as a visual cue to illustrate the value for each control. The color coding is only intended to reinforce the underlying Collaboration Index value for each control and not to provide additional guidance.

Janet Ríos Colón

Digitally signed by Janet Ríos Colón
Date: 2024.03.13 12:41:37 -04'00'