TALATEK LLC
COMPLIANCE THROUGH RISK MANAGEMENT

NIST SP 800-53, Rev. 5

Security and Privacy Controls for Information Systems and Organizations

Draft – December 2017

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
AC-1	ACCESS CONTROL POLICY AND PROCEDURES				A	O	x	x	x
AC-2	ACCOUNT MANAGEMENT					O	x	x	x
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT					O		x	x
AC-2(2)	REMOVAL OF TEMPORARY AND EMERGENCY ACCOUNTS					S		x	x
AC-2(3)	DISABLE ACCOUNTS					S		x	x
AC-2(4)	AUTOMATED AUDIT ACTIONS					S		x	x
AC-2(5)	INACTIVITY LOGOUT					O/S		x	x
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT					S			
AC-2(7)	ROLE-BASED SCHEMES					O			
AC-2(8)	DYNAMIC ACCOUNT MANAGEMENT					S			
AC-2(9)	RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS					O			
AC-2(10)	SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE					O		x	x
AC-2(11)	USAGE CONDITIONS					S			x
AC-2(12)	ACCOUNT MONITORING FOR ATYPICAL USAGE					O			x
AC-2(13)	DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS					O		x	x
AC-2(14)	PROHIBIT SPECIFIC ACCOUNT TYPES					O			
AC-2(15)	ATTRIBUTE-BASED SCHEMES					O			
AC-3	ACCESS ENFORCEMENT					S	x	x	x
AC-3(1)	RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS	W		Incorporated into AC-6.					
AC-3(2)	DUAL AUTHORIZATION					S			
AC-3(3)	MANDATORY ACCESS CONTROL					S			
AC-3(4)	DISCRETIONARY ACCESS CONTROL					S			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
AC-3(5)	SECURITY-RELEVANT INFORMATION					S			
AC-3(6)	PROTECTION OF USER AND SYSTEM INFORMATION	W	Incorporated into MP-4, SC-28.						
AC-3(7)	ROLE-BASED ACCESS CONTROL					O/S			
AC-3(8)	REVOCATION OF ACCESS AUTHORIZATIONS					O/S			
AC-3(9)	CONTROLLED RELEASE					O/S			
AC-3(10)	AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS					O			
AC-3(11)	RESTRICT ACCESS TO SPECIFIC INFORMATION					S			
AC-3(12)	ASSERT AND ENFORCE APPLICATION ACCESS					S			
AC-3(13)	ATTRIBUTE-BASED ACCESS CONTROL					S			
AC-4	INFORMATION FLOW ENFORCEMENT					S		x	x
AC-4(1)	OBJECT SECURITY 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			x
AC-4(5)	EMBEDDED DATA TYPES					S			
AC-4(6)	METADATA					S			
AC-4(7)	ONE-WAY FLOW MECHANISMS					S			
AC-4(8)	SECURITY POLICY FILTERS					S			
AC-4(9)	HUMAN REVIEWS					O			
AC-4(10)	ENABLE AND DISABLE SECURITY POLICY FILTERS					S			
AC-4(11)	CONFIGURATION OF SECURITY POLICY FILTERS					S			
AC-4(12)	DATA TYPE IDENTIFIERS					S			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
AC-4(13)	DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS					S			
AC-4(14)	SECURITY POLICY FILTER CONSTRAINTS					S			
AC-4(15)	DETECTION OF UNSANCTIONED INFORMATION					S			
AC-4(16)	INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS	W	Incorporated into AC-4.						
AC-4(17)	DOMAIN AUTHENTICATION					S			
AC-4(18)	SECURITY ATTRIBUTE BINDING	W	Incorporated into AC-16.						
AC-4(19)	VALIDATION OF METADATA					S			
AC-4(20)	APPROVED SOLUTIONS					O			
AC-4(21)	PHYSICAL AND LOGICAL SEPARATION OF INFORMATION FLOWS					S			
AC-4(22)	ACCESS ONLY					S			
AC-5	SEPARATION OF DUTIES					O		x	x
AC-6	LEAST PRIVILEGE					O		x	x
AC-6(1)	AUTHORIZE ACCESS TO SECURITY FUNCTIONS					O		x	x
AC-6(2)	NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS					O		x	x
AC-6(3)	NETWORK ACCESS TO PRIVILEGED COMMANDS					O			x
AC-6(4)	SEPARATE PROCESSING DOMAINS					S			
AC-6(5)	PRIVILEGED ACCOUNTS					O		x	x
AC-6(6)	PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS					O			
AC-6(7)	REVIEW OF USER PRIVILEGES					O	x	x	x
AC-6(8)	PRIVILEGE LEVELS FOR CODE EXECUTION					S			
AC-6(9)	AUDITING USE OF PRIVILEGED FUNCTIONS					S	x	x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
AC-6(10)	PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS					S		x	x
AC-7	UNSUCCESSFUL LOGON ATTEMPTS					S	x	x	x
AC-7(1)	AUTOMATIC ACCOUNT LOCK	W	Incorporated into AC-7.						
AC-7(2)	PURGE OR WIPE MOBILE DEVICE					S			
AC-7(3)	BIOMETRIC ATTEMPT LIMITING					O			
AC-7(4)	USE OF ALTERNATE FACTOR					O			
AC-8	SYSTEM USE NOTIFICATION					O/S	x	x	x
AC-9	PREVIOUS LOGON (ACCESS) 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			x
AC-11	DEVICE LOCK					S		x	x
AC-11(1)	PATTERN-HIDING DISPLAYS					S		x	x
AC-11(2)	REQUIRE USER-INITIATED LOCK					O			
AC-12	SESSION TERMINATION					S		x	x
AC-12(1)	USER-INITIATED LOGOUTS					O			
AC-12(2)	TERMINATION MESSAGE					S			
AC-12(3)	TIMEOUT WARNING MESSAGE					S			
AC-13	SUPERVISION AND REVIEW — ACCESS CONTROL	W	Incorporated into AC-2, AU-6.						
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION					O	x	x	x
AC-14(1)	NECESSARY USES	W	Incorporated into AC-14.						

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
AC-15	AUTOMATED MARKING	W	Incorporated into MP-3.						
AC-16	SECURITY AND PRIVACY ATTRIBUTES		P	D		O			
AC-16(1)	DYNAMIC ATTRIBUTE ASSOCIATION		P	D		S			
AC-16(2)	ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS		P	D		S			
AC-16(3)	MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM		P	D		S			
AC-16(4)	ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS		P	D		S			
AC-16(5)	ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES		P	D		S			
AC-16(6)	MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION		P	D		O			
AC-16(7)	CONSISTENT ATTRIBUTE INTERPRETATION		P	D		O			
AC-16(8)	ASSOCIATION TECHNIQUES AND TECHNOLOGIES		P	D		S			
AC-16(9)	ATTRIBUTE REASSIGNMENT		P	D		O			
AC-16(10)	ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS		P	D		O			
AC-16(11)	AUDIT CHANGES		P	D		S			
AC-17	REMOTE ACCESS					O	x	x	x
AC-17(1)	AUTOMATED MONITORING AND CONTROL					S		x	x
AC-17(2)	PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION					S		x	x
AC-17(3)	MANAGED ACCESS CONTROL POINTS					S		x	x
AC-17(4)	PRIVILEGED COMMANDS AND ACCESS					O		x	x
AC-17(5)	MONITORING FOR UNAUTHORIZED CONNECTIONS	W	Incorporated into SI-4.						
AC-17(6)	PROTECTION OF INFORMATION					O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
AC-17(7)	ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS	W	Incorporated into AC-3(10).						
AC-17(8)	DISABLE NONSECURE NETWORK PROTOCOLS	W	Incorporated into CM-7.						
AC-17(9)	DISCONNECT OR DISABLE ACCESS					O			
AC-18	WIRELESS ACCESS					O	x	x	x
AC-18(1)	AUTHENTICATION AND ENCRYPTION					S		x	x
AC-18(2)	MONITORING UNAUTHORIZED CONNECTIONS	W	Incorporated into SI-4.						
AC-18(3)	DISABLE WIRELESS NETWORKING					O/S		x	x
AC-18(4)	RESTRICT CONFIGURATIONS BY USERS					O			x
AC-18(5)	ANTENNAS AND TRANSMISSION POWER LEVELS					O			x
AC-19	ACCESS CONTROL FOR MOBILE DEVICES					O	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					O			
AC-19(5)	FULL DEVICE AND CONTAINER-BASED ENCRYPTION					O		x	x
AC-20	USE OF EXTERNAL SYSTEMS					O	x	x	x
AC-20(1)	LIMITS ON AUTHORIZED USE					O		x	x
AC-20(2)	PORTABLE STORAGE DEVICES					O		x	x
AC-20(3)	NON-ORGANIZATIONALLY OWNED SYSTEMS AND COMPONENTS					O			
AC-20(4)	NETWORK ACCESSIBLE STORAGE DEVICES					O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
AC-21	INFORMATION SHARING		P	D		O		x	x
AC-21(1)	AUTOMATED DECISION SUPPORT					S			
AC-21(2)	INFORMATION SEARCH AND RETRIEVAL					S			
AC-22	PUBLICLY ACCESSIBLE CONTENT					O	x	x	x
AC-23	DATA MINING PROTECTION		P	D		O			
AC-24	ACCESS CONTROL DECISIONS					O			
AC-24(1)	TRANSMIT ACCESS AUTHORIZATION INFORMATION					S			
AC-24(2)	NO USER OR PROCESS IDENTITY					S			
AC-25	REFERENCE MONITOR				A	S			
AWARENESS AND TRAINING (AT)									
AT-1	AWARENESS AND TRAINING POLICY AND PROCEDURES		P	R	A	O	x	x	x
AT-2	AWARENESS TRAINING		P	R	A	O	x	x	x
AT-2(1)	PRACTICAL EXERCISES		P	D	A	O			
AT-2(2)	INSIDER THREAT				A	O	x	x	x
AT-2(3)	SOCIAL ENGINEERING AND MINING				A	O		x	x
AT-3	ROLE-BASED TRAINING		P	R	A	O	x	x	x
AT-3(1)	ENVIRONMENTAL CONTROLS				A	O			
AT-3(2)	PHYSICAL SECURITY CONTROLS				A	O			
AT-3(3)	PRACTICAL EXERCISES		P	D	A	O			
AT-3(4)	SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR				A	O			
AT-3(5)	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING		P	R	A	O			
AT-4	TRAINING RECORDS		P	R	A	O	x	x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
AT-5	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	W	Incorporated into PM-15.						
AUDIT AND ACCOUNTABILITY (AU)									
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES				A	O	x	x	x
AU-2	AUDIT EVENTS					O	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					O		x	x
AU-2(4)	PRIVILEGED FUNCTIONS	W	Incorporated into AC-6(9).						
AU-3	CONTENT OF AUDIT RECORDS					S	x	x	x
AU-3(1)	ADDITIONAL AUDIT INFORMATION					S		x	x
AU-3(2)	CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT					S			x
AU-3(3)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS		P	D		O			
AU-4	AUDIT STORAGE CAPACITY					O/S	x	x	x
AU-4(1)	TRANSFER TO ALTERNATE STORAGE					O			
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES					S	x	x	x
AU-5(1)	AUDIT STORAGE CAPACITY					S			x
AU-5(2)	REAL-TIME ALERTS					S			x
AU-5(3)	CONFIGURABLE TRAFFIC VOLUME THRESHOLDS					S			
AU-5(4)	SHUTDOWN ON FAILURE					S			
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING				A	O	x	x	x
AU-6(1)	AUTOMATED PROCESS INTEGRATION				A	O		x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
AU-6(2)	AUTOMATED SECURITY ALERTS	W	Incorporated into SI-4.						
AU-6(3)	CORRELATE AUDIT REPOSITORIES				A	O		x	x
AU-6(4)	CENTRAL REVIEW AND ANALYSIS				A	S			
AU-6(5)	INTEGRATED ANALYSIS OF AUDIT RECORDS				A	O			x
AU-6(6)	CORRELATION WITH PHYSICAL MONITORING				A	O			x
AU-6(7)	PERMITTED ACTIONS				A	O			
AU-6(8)	FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS				A	O			
AU-6(9)	CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES				A	O			
AU-6(10)	AUDIT LEVEL ADJUSTMENT	W	Incorporated into AU-6.						
AU-7	AUDIT REDUCTION AND REPORT GENERATION				A	S		x	x
AU-7(1)	AUTOMATIC PROCESSING				A	S		x	x
AU-7(2)	AUTOMATIC SORT AND SEARCH					S			
AU-8	TIME STAMPS					S	x	x	x
AU-8(1)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE					S		x	x
AU-8(2)	SECONDARY AUTHORITATIVE TIME SOURCE					S			
AU-9	PROTECTION OF AUDIT INFORMATION					S	x	x	x
AU-9(1)	HARDWARE WRITE-ONCE MEDIA					S			
AU-9(2)	STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS					S			x
AU-9(3)	CRYPTOGRAPHIC PROTECTION					S			x
AU-9(4)	ACCESS BY SUBSET OF PRIVILEGED USERS					O		x	x
AU-9(5)	DUAL AUTHORIZATION					O/S			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
AU-9(6)	READ-ONLY ACCESS					O/S			
AU-9(7)	STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM					O			
AU-10	NON-REPUDIATION				A	S			x
AU-10(1)	ASSOCIATION OF IDENTITIES				A	S			
AU-10(2)	VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY				A	S			
AU-10(3)	CHAIN OF CUSTODY				A	O/S			
AU-10(4)	VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY				A	S			
AU-10(5)	DIGITAL SIGNATURES	W	Incorporated into SI-7.						
AU-11	AUDIT RECORD RETENTION		P	R		O	x	x	x
AU-11(1)	LONG-TERM RETRIEVAL CAPABILITY				A	O			
AU-12	AUDIT GENERATION					S	x	x	x
AU-12(1)	SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL					S			x
AU-12(2)	STANDARDIZED FORMATS					S			
AU-12(3)	CHANGES BY AUTHORIZED INDIVIDUALS					S			x
AU-12(4)	QUERY PARAMETER AUDITS OF PERSONALLY IDENTIFIABLE INFORMATION		P	D		S			
AU-13	MONITORING FOR INFORMATION DISCLOSURE				A	O			
AU-13(1)	USE OF AUTOMATED TOOLS				A	O/S			
AU-13(2)	REVIEW OF MONITORED SITES				A	O			
AU-14	SESSION AUDIT				A	S			
AU-14(1)	SYSTEM START-UP				A	S			
AU-14(2)	CAPTURE AND RECORD CONTENT				A	S			
AU-14(3)	REMOTE VIEWING AND LISTENING				A	S			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
AU-15	ALTERNATE AUDIT CAPABILITY					O			
AU-16	CROSS-ORGANIZATIONAL AUDITING		P	D		O			
AU-16(1)	IDENTITY PRESERVATION					O			
AU-16(2)	SHARING OF AUDIT INFORMATION					O			
ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)									
CA-1	ASSESSMENT, AUTHORIZATION, AND MONITORING POLICIES AND PROCEDURES		P	R	A	O	x	x	x
CA-2	ASSESSMENTS		P	R	A	O	x	x	x
CA-2(1)	INDEPENDENT ASSESSORS		P	D	A	O		x	x
CA-2(2)	SPECIALIZED ASSESSMENTS				A	O			x
CA-2(3)	EXTERNAL ORGANIZATIONS		P	D	A	O			
CA-3	SYSTEM INTERCONNECTIONS				A	O	x	x	x
CA-3(1)	UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS					O			
CA-3(2)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS					O			
CA-3(3)	UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS					O			
CA-3(4)	CONNECTIONS TO PUBLIC NETWORKS					O			
CA-3(5)	RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS					O		x	x
CA-3(6)	SECONDARY AND TERTIARY CONNECTIONS					O			x
CA-4	SECURITY CERTIFICATION	W	Incorporated into CA-2.						
CA-5	PLAN OF ACTION AND MILESTONES		P	R	A	O	x	x	x
CA-5(1)	AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY				A	O			
CA-6	AUTHORIZATION				A	O	x	x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
CA-6(1)	JOINT AUTHORIZATION — SAME ORGANIZATION				A	O			
CA-6(2)	JOINT AUTHORIZATION — DIFFERENT ORGANIZATIONS				A	O			
CA-7	CONTINUOUS MONITORING		P	R	A	O	x	x	x
CA-7(1)	INDEPENDENT ASSESSMENT		P	D	A	O		x	x
CA-7(2)	TYPES OF ASSESSMENTS	W		Incorporated into CA-2.					
CA-7(3)	TREND ANALYSES				A	O			
CA-7(4)	RISK MONITORING				A		x	x	x
CA-8	PENETRATION TESTING				A	O			x
CA-8(1)	INDEPENDENT PENETRATION AGENT OR TEAM				A	O			x
CA-8(2)	RED TEAM EXERCISES				A	O			
CA-8(3)	FACILITY PENETRATION TESTING				A	O			
CA-9	INTERNAL SYSTEM CONNECTIONS				X	O	x	x	x
CA-9(1)	COMPLIANCE CHECKS				X	S			

CONFIGURATION MANAGEMENT (CM)

CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES		P	R	A	O	x	x	x
CM-2	BASELINE CONFIGURATION				A	O	x	x	x
CM-2(1)	REVIEWS AND UPDATES	W		Incorporated into CM-2.					
CM-2(2)	AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY				A	O		x	x
CM-2(3)	RETENTION OF PREVIOUS CONFIGURATIONS				A	O		x	x
CM-2(4)	UNAUTHORIZED SOFTWARE	W		Incorporated into CM-7.					
CM-2(5)	AUTHORIZED SOFTWARE	W		Incorporated into CM-7.					

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
CM-2(6)	DEVELOPMENT AND TEST ENVIRONMENTS				A	O			
CM-2(7)	CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS				A	O		x	x
CM-3	CONFIGURATION CHANGE CONTROL				A	O		x	x
CM-3(1)	AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES				A	O			x
CM-3(2)	TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES				A	O		x	x
CM-3(3)	AUTOMATED CHANGE IMPLEMENTATION					O			
CM-3(4)	SECURITY REPRESENTATIVE					O		x	x
CM-3(5)	AUTOMATED SECURITY RESPONSE					S			
CM-3(6)	CRYPTOGRAPHY MANAGEMENT					O			x
CM-4	SECURITY AND PRIVACY IMPACT ANALYSES		P	R	A	O	x	x	x
CM-4(1)	SEPARATE TEST ENVIRONMENTS				A	O			x
CM-4(2)	VERIFICATION OF SECURITY AND PRIVACY FUNCTIONS		P	D	A	O		x	x
CM-5	ACCESS RESTRICTIONS FOR CHANGE					O	x	x	x
CM-5(1)	AUTOMATED ACCESS ENFORCEMENT AND AUDITING					S			x
CM-5(2)	REVIEW SYSTEM CHANGES					O			x
CM-5(3)	SIGNED COMPONENTS					O/S			x
CM-5(4)	DUAL AUTHORIZATION					O/S			
CM-5(5)	PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION					O			
CM-5(6)	LIMIT LIBRARY PRIVILEGES					O			
CM-5(7)	AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS	W	Incorporated into SI-7.						
CM-6	CONFIGURATION SETTINGS					O	x	x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
CM-6(1)	AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION					O			x
CM-6(2)	RESPOND TO UNAUTHORIZED CHANGES					O			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					O	x	x	x
CM-7(1)	PERIODIC REVIEW					O		x	x
CM-7(2)	PREVENT PROGRAM EXECUTION					S		x	x
CM-7(3)	REGISTRATION COMPLIANCE					O			
CM-7(4)	UNAUTHORIZED SOFTWARE — BLACKLISTING					O			
CM-7(5)	AUTHORIZED SOFTWARE — WHITELISTING					O		x	x
CM-8	SYSTEM COMPONENT INVENTORY				A	O	x	x	x
CM-8(1)	UPDATES DURING INSTALLATION AND REMOVAL				A	O		x	x
CM-8(2)	AUTOMATED MAINTENANCE				A	O			x
CM-8(3)	AUTOMATED UNAUTHORIZED COMPONENT DETECTION				A	O		x	x
CM-8(4)	ACCOUNTABILITY INFORMATION				A	O			x
CM-8(5)	NO DUPLICATE ACCOUNTING OF COMPONENTS				A	O			
CM-8(6)	ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS				A	O			
CM-8(7)	CENTRALIZED REPOSITORY				A	O			
CM-8(8)	AUTOMATED LOCATION TRACKING				A	O			
CM-8(9)	ASSIGNMENT OF COMPONENTS TO SYSTEMS				A	O			
CM-8(10)	DATA ACTION MAPPING		P	D	A	O			
CM-9	CONFIGURATION MANAGEMENT PLAN					O		x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
CM-9(1)	ASSIGNMENT OF RESPONSIBILITY					O			
CM-10	SOFTWARE USAGE RESTRICTIONS					O	x	x	x
CM-10(1)	OPEN SOURCE SOFTWARE					O			
CM-11	USER-INSTALLED SOFTWARE					O	x	x	x
CM-11(1)	ALERTS FOR UNAUTHORIZED INSTALLATIONS	W	Incorporated into CM-8(3).						
CM-11(2)	SOFTWARE INSTALLATION WITH PRIVILEGED STATUS					S			
CM-12	INFORMATION LOCATION		P	D	A	O		x	x
CM-12(1)	AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION		P	D	A	O		x	x

CONTINGENCY PLANNING (CP)

CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES		P	R	A	O	x	x	x
CP-2	CONTINGENCY PLAN		P	R		O	x	x	x
CP-2(1)	COORDINATE WITH RELATED PLANS		P	D		O		x	x
CP-2(2)	CAPACITY PLANNING					O			x
CP-2(3)	RESUME ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS		P	D		O		x	x
CP-2(4)	RESUME ALL MISSIONS AND BUSINESS FUNCTIONS		P	D		O			x
CP-2(5)	CONTINUE ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS		P	D		O			x
CP-2(6)	ALTERNATE PROCESSING AND STORAGE SITES					O			
CP-2(7)	COORDINATE WITH EXTERNAL SERVICE PROVIDERS		P	D		O			
CP-2(8)	IDENTIFY CRITICAL ASSETS		P	D		O		x	x
CP-3	CONTINGENCY TRAINING		P	S	A	O	x	x	x
CP-3(1)	SIMULATED EVENTS		P	D	A	O			x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
CP-3(2)	AUTOMATED TRAINING ENVIRONMENTS		P	D	A	O			
CP-4	CONTINGENCY PLAN TESTING		P	R	A	O	x	x	x
CP-4(1)	COORDINATE WITH RELATED PLANS		P	D	A	O		x	x
CP-4(2)	ALTERNATE PROCESSING SITE				A	O			x
CP-4(3)	AUTOMATED TESTING				A	O			
CP-4(4)	FULL RECOVERY AND RECONSTITUTION				A	O			
CP-5	CONTINGENCY PLAN UPDATE	W	Incorporated into CP-2.						
CP-6	ALTERNATE STORAGE SITE					O		x	x
CP-6(1)	SEPARATION FROM PRIMARY SITE					O		x	x
CP-6(2)	RECOVERY TIME AND RECOVERY POINT OBJECTIVES					O			x
CP-6(3)	ACCESSIBILITY					O		x	x
CP-7	ALTERNATE PROCESSING SITE					O		x	x
CP-7(1)	SEPARATION FROM PRIMARY SITE					O		x	x
CP-7(2)	ACCESSIBILITY					O		x	x
CP-7(3)	PRIORITY OF SERVICE					O		x	x
CP-7(4)	PREPARATION FOR USE					O			x
CP-7(5)	EQUIVALENT INFORMATION SECURITY SAFEGUARDS	W	Incorporated into CP-7.						
CP-7(6)	INABILITY TO RETURN TO PRIMARY SITE					O			
CP-8	TELECOMMUNICATIONS SERVICES					O		x	x
CP-8(1)	PRIORITY OF SERVICE PROVISIONS					O		x	x
CP-8(2)	SINGLE POINTS OF FAILURE					O		x	x
CP-8(3)	SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS					O			x
CP-8(4)	PROVIDER CONTINGENCY PLAN					O			x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
CP-8(5)	ALTERNATE TELECOMMUNICATION SERVICE TESTING					O			
CP-9	SYSTEM BACKUP					O	x	x	x
CP-9(1)	TESTING FOR RELIABILITY AND INTEGRITY					O		x	x
CP-9(2)	TEST RESTORATION USING SAMPLING					O			x
CP-9(3)	SEPARATE STORAGE FOR CRITICAL INFORMATION					O			x
CP-9(4)	PROTECTION FROM UNAUTHORIZED MODIFICATION	W		Incorporated into CP-9.					
CP-9(5)	TRANSFER TO ALTERNATE STORAGE SITE					O			x
CP-9(6)	REDUNDANT SECONDARY SYSTEM					O			
CP-9(7)	DUAL AUTHORIZATION					O			
CP-9(8)	CRYPTOGRAPHIC PROTECTION					O		x	x
CP-10	SYSTEM RECOVERY AND RECONSTITUTION					O	x	x	x
CP-10(1)	CONTINGENCY PLAN TESTING	W		Incorporated into CP-4.					
CP-10(2)	TRANSACTION RECOVERY					O		x	x
CP-10(3)	COMPENSATING SECURITY CONTROLS	W		Incorporated into PL-11.					
CP-10(4)	RESTORE WITHIN TIME-PERIOD					O			x
CP-10(5)	FAILOVER CAPABILITY	W		Incorporated into SI-13.					
CP-10(6)	COMPONENT PROTECTION					O			
CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS					O			
CP-12	SAFE MODE				A	S			
CP-13	ALTERNATIVE SECURITY MECHANISMS					O/S			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES		P	D	A	O	x	x	x
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)					O/S	x	x	x
IA-2(1)	MULTIFACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS					S	x	x	x
IA-2(2)	MULTIFACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS					S	x	x	x
IA-2(3)	LOCAL ACCESS TO PRIVILEGED ACCOUNTS	W	Incorporated into IA-2(1)(2).						
IA-2(4)	LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS	W	Incorporated into IA-2(1)(2).						
IA-2(5)	INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION					O			x
IA-2(6)	NETWORK ACCESS TO PRIVILEGED ACCOUNTS — SEPARATE DEVICE	W	Incorporated into IA-2(1)(2).						
IA-2(7)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — SEPARATE DEVICE	W	Incorporated into IA-2(1)(2).						
IA-2(8)	ACCESS TO ACCOUNTS — REPLAY RESISTANT					S	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					S			
IA-2(11)	REMOTE ACCESS — SEPARATE DEVICE	W	Incorporated into IA-2(1)(2).						
IA-2(12)	ACCEPTANCE OF PIV CREDENTIALS					S	x	x	x
IA-2(13)	OUT-OF-BAND AUTHENTICATION	W	Incorporated into IA-2(1)(2).						
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION					S		x	x
IA-3(1)	CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION					S			
IA-3(2)	CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION	W	Incorporated into IA-3(1).						

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
IA-3(3)	DYNAMIC ADDRESS ALLOCATION					O			
IA-3(4)	DEVICE ATTESTATION					O			
IA-4	IDENTIFIER MANAGEMENT					O	x	x	x
IA-4(1)	PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS					O			
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		P	D		O		x	x
IA-4(5)	DYNAMIC MANAGEMENT					S			
IA-4(6)	CROSS-ORGANIZATION MANAGEMENT					O			
IA-4(7)	IN-PERSON REGISTRATION	W	Incorporated into IA-12(4).						
IA-4(8)	PAIRWISE PSEUDONYMOUS IDENTIFIERS		P	D		O			
IA-5	AUTHENTICATOR MANAGEMENT					O	x	x	x
IA-5(1)	PASSWORD-BASED AUTHENTICATION					O/S	x	x	x
IA-5(2)	PUBLIC KEY-BASED AUTHENTICATION					S		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					O			
IA-5(6)	PROTECTION OF AUTHENTICATORS					O		x	x
IA-5(7)	NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS					O			
IA-5(8)	MULTIPLE SYSTEM ACCOUNTS					O			
IA-5(9)	FEDERATED CREDENTIAL MANAGEMENT					O			
IA-5(10)	DYNAMIC CREDENTIAL BINDING					S			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
IA-5(11)	HARDWARE TOKEN-BASED AUTHENTICATION	W	Incorporated into IA-2(1)(2).						
IA-5(12)	BIOMETRIC AUTHENTICATION PERFORMANCE					S			
IA-5(13)	EXPIRATION OF CACHED AUTHENTICATORS					S			
IA-5(14)	MANAGING CONTENT OF PKI TRUST STORES					O			
IA-5(15)	GSA-APPROVED PRODUCTS AND SERVICES					O			
IA-5(16)	IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE					O			
IA-5(17)	PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS					S			
IA-6	AUTHENTICATOR FEEDBACK					S	x	x	x
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION					S	x	x	x
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)					S	x	x	x
IA-8(1)	ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES					S	x	x	x
IA-8(2)	ACCEPTANCE OF EXTERNAL PARTY CREDENTIALS					S	x	x	x
IA-8(3)	USE OF FICAM-APPROVED PRODUCTS	W	Incorporated into IA-8(2).						
IA-8(4)	USE OF NIST-ISSUED PROFILES					S	x	x	x
IA-8(5)	ACCEPTANCE OF PIV-I CREDENTIALS					S			
IA-8(6)	DISASSOCIABILITY		P	D		O			
IA-9	SERVICE IDENTIFICATION AND AUTHENTICATION					O/S			
IA-9(1)	INFORMATION EXCHANGE					O			
IA-9(2)	TRANSMISSION OF DECISIONS					O			
IA-10	ADAPTIVE AUTHENTICATION					O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
IA-11	RE-AUTHENTICATION					O/S	x	x	x
IA-12	IDENTITY PROOFING					O		x	x
IA-12(1)	SUPERVISOR AUTHORIZATION					O			
IA-12(2)	IDENTITY EVIDENCE					O		x	x
IA-12(3)	IDENTITY EVIDENCE VALIDATION AND VERIFICATION					O		x	x
IA-12(4)	IN-PERSON VALIDATION AND VERIFICATION					O			x
IA-12(5)	ADDRESS CONFIRMATION					O		x	x
IA-12(6)	ACCEPT EXTERNALLY PROOFED IDENTITIES					O			
INDIVIDUAL PARTICIPATION (IP)									
IP-1	INDIVIDUAL PARTICIPATION POLICY AND PROCEDURES		P	R		O			
IP-2	CONSENT		P	S		O			
IP-2(1)	ATTRIBUTE MANAGEMENT		P	D		O			
IP-2(2)	JUST-IN-TIME NOTICE OF CONSENT		P	D		O			
IP-3	REDRESS		P	S		O			
IP-3(1)	NOTICE OF CORRECTION OR AMENDMENT		P	S		O			
IP-3(2)	APPEAL		P	S		O			
IP-4	PRIVACY NOTICE		P	S		O			
IP-4(1)	JUST-IN-TIME NOTICE OF PRIVACY AUTHORIZATION		P	D		O			
IP-5	PRIVACY ACT STATEMENTS		P	S		O			
IP-6	INDIVIDUAL ACCESS		P	S		O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES		P	R	A	O	x	x	x
IR-2	INCIDENT RESPONSE TRAINING		P	R	A	O	x	x	x
IR-2(1)	SIMULATED EVENTS		P	D	A	O			x
IR-2(2)	AUTOMATED TRAINING ENVIRONMENTS		P	D	A	O			x
IR-3	INCIDENT RESPONSE TESTING		P	D	A	O		x	x
IR-3(1)	AUTOMATED TESTING				A	O			
IR-3(2)	COORDINATION WITH RELATED PLANS		P	D	A	O		x	x
IR-3(3)	CONTINUOUS IMPROVEMENT				A	O			
IR-4	INCIDENT HANDLING		P	R		O	x	x	x
IR-4(1)	AUTOMATED INCIDENT HANDLING PROCESSES					O		x	x
IR-4(2)	DYNAMIC RECONFIGURATION					O			
IR-4(3)	CONTINUITY OF OPERATIONS					O			
IR-4(4)	INFORMATION CORRELATION					O			x
IR-4(5)	AUTOMATIC DISABLING OF SYSTEM					O/S			
IR-4(6)	INSIDER THREATS — SPECIFIC CAPABILITIES					O			
IR-4(7)	INSIDER THREATS — INTRA-ORGANIZATION COORDINATION					O			
IR-4(8)	CORRELATION WITH EXTERNAL ORGANIZATIONS					O			
IR-4(9)	DYNAMIC RESPONSE CAPABILITY					O			
IR-4(10)	SUPPLY CHAIN COORDINATION					O			
IR-5	INCIDENT MONITORING		P	R	A	O	x	x	x
IR-5(1)	AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS		P	D	A	O			x
IR-6	INCIDENT REPORTING		P	R		O	x	x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
IR-6(1)	AUTOMATED REPORTING					O		x	x
IR-6(2)	VULNERABILITIES RELATED TO INCIDENTS					O			
IR-6(3)	SUPPLY CHAIN COORDINATION					O		x	x
IR-7	INCIDENT RESPONSE ASSISTANCE		P	R		O	x	x	x
IR-7(1)	AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT					O		x	x
IR-7(2)	COORDINATION WITH EXTERNAL PROVIDERS					O			
IR-8	INCIDENT RESPONSE PLAN		P	R		O	x	x	x
IR-8(1)	PERSONALLY IDENTIFIABLE INFORMATION PROCESSES		P	S		O			
IR-9	INFORMATION SPILLAGE RESPONSE		P	D		O			
IR-9(1)	RESPONSIBLE PERSONNEL					O			
IR-9(2)	TRAINING					O			
IR-9(3)	POST-SPILL OPERATIONS					O			
IR-9(4)	EXPOSURE TO UNAUTHORIZED PERSONNEL					O			
IR-10	INTEGRATED INFORMATION SECURITY ANALYSIS TEAM					O			x
MAINTENANCE (MA)									
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES				A	O	x	x	x
MA-2	CONTROLLED MAINTENANCE					O	x	x	x
MA-2(1)	RECORD CONTENT	W	Incorporated into MA-2.						
MA-2(2)	AUTOMATED MAINTENANCE ACTIVITIES					O			x
MA-3	MAINTENANCE TOOLS					O		x	x
MA-3(1)	INSPECT TOOLS					O		x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
MA-3(2)	INSPECT MEDIA					O		x	x
MA-3(3)	PREVENT UNAUTHORIZED REMOVAL					O		x	x
MA-3(4)	RESTRICTED TOOL USE					S			
MA-4	NONLOCAL MAINTENANCE					O	x	x	x
MA-4(1)	AUDITING AND REVIEW					O			
MA-4(2)	DOCUMENT NONLOCAL MAINTENANCE	W	Incorporated into MA-1, MA-4.						
MA-4(3)	COMPARABLE SECURITY AND SANITIZATION					O			x
MA-4(4)	AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS					O			
MA-4(5)	APPROVALS AND NOTIFICATIONS					O			
MA-4(6)	CRYPTOGRAPHIC PROTECTION					O/S			
MA-4(7)	REMOTE DISCONNECT VERIFICATION					S			
MA-5	MAINTENANCE PERSONNEL					O	x	x	x
MA-5(1)	INDIVIDUALS WITHOUT APPROPRIATE ACCESS					O			x
MA-5(2)	SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS					O			
MA-5(3)	CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS					O			
MA-5(4)	FOREIGN NATIONALS					O			
MA-5(5)	NON-SYSTEM MAINTENANCE					O			
MA-6	TIMELY MAINTENANCE					O		x	x
MA-6(1)	PREVENTIVE MAINTENANCE					O			
MA-6(2)	PREDICTIVE MAINTENANCE					O			
MA-6(3)	AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE					O			
MA-6(4)	ADEQUATE SUPPLY					O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES				A	O	x	x	x
MP-2	MEDIA ACCESS					O	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					O		x	x
MP-4	MEDIA STORAGE					O		x	x
MP-4(1)	CRYPTOGRAPHIC PROTECTION	W	Incorporated into SC-28(1).						
MP-4(2)	AUTOMATED RESTRICTED ACCESS					O			
MP-5	MEDIA TRANSPORT					O		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					O			
MP-5(4)	CRYPTOGRAPHIC PROTECTION	W	Incorporated into SC-28(1).						
MP-6	MEDIA SANITIZATION					O	x	x	x
MP-6(1)	REVIEW, APPROVE, TRACK, DOCUMENT, VERIFY					O			x
MP-6(2)	EQUIPMENT TESTING					O			x
MP-6(3)	NONDESTRUCTIVE TECHNIQUES					O			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					O			
MP-6(8)	REMOTE PURGING OR WIPING OF INFORMATION					O			
MP-6(9)	DESTRUCTION OF PERSONALLY IDENTIFIABLE INFORMATION			S		O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
MP-7	MEDIA USE					O	x	x	x
MP-7(1)	PROHIBIT USE WITHOUT OWNER	W		Incorporated into MP-7.					
MP-7(2)	PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA					O			
MP-8	MEDIA DOWNGRADING					O			
MP-8(1)	DOCUMENTATION OF PROCESS					O			
MP-8(2)	EQUIPMENT TESTING					O			
MP-8(3)	CONTROLLED UNCLASSIFIED INFORMATION					O			
MP-8(4)	CLASSIFIED INFORMATION					O			
PRIVACY AUTHORIZATION (PA)									
PA-1	PRIVACY AUTHORIZATION POLICY AND PROCEDURES		P	R		O			
PA-2	AUTHORITY TO COLLECT		P	S		O			
PA-3	PURPOSE SPECIFICATION		P	S		O			
PA-3(1)	USAGE RESTRICTIONS OF PERSONALLY IDENTIFIABLE INFORMATION		P	R		O			
PA-3(2)	AUTOMATION		P	D		S			
PA-4	INFORMATION SHARING WITH EXTERNAL PARTIES		P	S		O			
PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)									
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES				A	O	x	x	x
PE-2	PHYSICAL ACCESS AUTHORIZATIONS					O	x	x	x
PE-2(1)	ACCESS BY POSITION AND ROLE					O			
PE-2(2)	TWO FORMS OF IDENTIFICATION					O			
PE-2(3)	RESTRICT UNESCORTED ACCESS					O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
PE-3	PHYSICAL ACCESS CONTROL					O	x	x	x
PE-3(1)	SYSTEM ACCESS					O			x
PE-3(2)	FACILITY AND SYSTEM BOUNDARIES					O			
PE-3(3)	CONTINUOUS GUARDS					O			
PE-3(4)	LOCKABLE CASINGS					O			
PE-3(5)	TAMPER PROTECTION					O			
PE-3(6)	FACILITY PENETRATION TESTING	W	Incorporated into CA-8.						
PE-3(7)	PHYSICAL BARRIERS					O			
PE-4	ACCESS CONTROL FOR TRANSMISSION					O		x	x
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES					O		x	x
PE-5(1)	ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS					O			
PE-5(2)	ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY					S			
PE-5(3)	MARKING OUTPUT DEVICES					O			
PE-6	MONITORING PHYSICAL ACCESS				A	O	x	x	x
PE-6(1)	INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT				A	O		x	x
PE-6(2)	AUTOMATED INTRUSION RECOGNITION AND RESPONSES				A	O			
PE-6(3)	VIDEO SURVEILLANCE				A	O			
PE-6(4)	MONITORING PHYSICAL ACCESS TO SYSTEMS				A	O			x
PE-7	VISITOR CONTROL	W	Incorporated into PE-2, PE-3.						
PE-8	VISITOR ACCESS RECORDS				A	O	x	x	x
PE-8(1)	AUTOMATED RECORDS MAINTENANCE AND REVIEW					O			x
PE-8(2)	PHYSICAL ACCESS RECORDS	W	Incorporated into PE-2.						

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
PE-9	POWER EQUIPMENT AND CABLING					O		x	x
PE-9(1)	REDUNDANT CABLING					O			
PE-9(2)	AUTOMATIC VOLTAGE CONTROLS					O			
PE-10	EMERGENCY SHUTOFF					O		x	x
PE-10(1)	ACCIDENTAL AND UNAUTHORIZED ACTIVATION	W	Incorporated into PE-10.						
PE-11	EMERGENCY POWER					O		x	x
PE-11(1)	LONG-TERM ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY					O			x
PE-11(2)	LONG-TERM ALTERNATE POWER SUPPLY — SELF-CONTAINED					O			
PE-12	EMERGENCY LIGHTING					O	x	x	x
PE-12(1)	ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS					O			
PE-13	FIRE PROTECTION					O	x	x	x
PE-13(1)	DETECTION DEVICES AND SYSTEMS					O		x	x
PE-13(2)	AUTOMATIC SUPPRESSION DEVICES AND SYSTEMS					O			x
PE-13(3)	AUTOMATIC FIRE SUPPRESSION	W	Incorporated into PE-13(2).						
PE-13(4)	INSPECTIONS					O			
PE-14	TEMPERATURE AND HUMIDITY CONTROLS					O	x	x	x
PE-14(1)	AUTOMATIC CONTROLS					O			
PE-14(2)	MONITORING WITH ALARMS AND NOTIFICATIONS					O			
PE-15	WATER DAMAGE PROTECTION					O	x	x	x
PE-15(1)	AUTOMATION SUPPORT					O			x
PE-16	DELIVERY AND REMOVAL					O	x	x	x
PE-17	ALTERNATE WORK SITE					O		x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
PE-18	LOCATION OF SYSTEM COMPONENTS					O			x
PE-18(1)	FACILITY SITE					O			
PE-19	INFORMATION LEAKAGE					O			
PE-19(1)	NATIONAL EMISSIONS AND TEMPEST POLICIES AND PROCEDURES					O			
PE-20	ASSET MONITORING AND TRACKING					O			
PE-21	ELECTROMAGNETIC PULSE PROTECTION					O			
PE-22	COMPONENT MARKING					O			
PLANNING (PL)									
PL-1	PLANNING POLICY AND PROCEDURES		P	R	A	O	x	x	x
PL-2	SECURITY AND PRIVACY PLANS		P	R	A	O	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		P	R	A	O		x	x
PL-3	SYSTEM SECURITY PLAN UPDATE	W	Incorporated into PL-2.						
PL-4	RULES OF BEHAVIOR		P	R	A	O	x	x	x
PL-4(1)	SOCIAL MEDIA AND NETWORKING RESTRICTIONS				A	O	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		P	D		O			
PL-8	SECURITY AND PRIVACY ARCHITECTURES		P	R	A	O		x	x
PL-8(1)	DEFENSE-IN-DEPTH				A	O			
PL-8(2)	SUPPLIER DIVERSITY		P	D	A	O			
PL-9	CENTRAL MANAGEMENT		P	R	A	O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
PL-10	BASELINE SELECTION					O	x	x	x
PL-11	BASELINE TAILORING					O	x	x	x
PROGRAM MANAGEMENT (PM)									
PM-1	INFORMATION SECURITY PROGRAM PLAN					O			
PM-2	INFORMATION SECURITY PROGRAM ROLES					O			
PM-3	INFORMATION SECURITY AND PRIVACY RESOURCES		P	R		O			
PM-4	PLAN OF ACTION AND MILESTONES PROCESS		P	R		O			
PM-5	SYSTEM INVENTORY					O			
PM-6	MEASURES OF PERFORMANCE		P	R	A	O			
PM-7	ENTERPRISE ARCHITECTURE		P	R		O			
PM-8	CRITICAL INFRASTRUCTURE PLAN		P	S		O			
PM-9	RISK MANAGEMENT STRATEGY		P	R	A	O			
PM-10	AUTHORIZATION PROCESS				A	O			
PM-11	MISSION AND BUSINESS PROCESS DEFINITION		P	R		O			
PM-12	INSIDER THREAT PROGRAM				A	O			
PM-13	SECURITY AND PRIVACY WORKFORCE		P	R		O			
PM-14	TESTING, TRAINING, AND MONITORING		P	R	A	O			
PM-15	CONTACTS WITH GROUPS AND ASSOCIATIONS		P	D		O			
PM-16	THREAT AWARENESS PROGRAM				A	O			
PM-16(1)	AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE				A	O			
PM-17	PROTECTING CUI ON EXTERNAL SYSTEMS				A	O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
PM-18	PRIVACY PROGRAM PLAN		P	R		O			
PM-19	PRIVACY PROGRAM ROLES		P	R		O			
PM-20	SYSTEM OF RECORDS NOTICE		P	S		O			
PM-21	DISSEMINATION OF PRIVACY PROGRAM INFORMATION		P	S		O			
PM-22	ACCOUNTING OF DISCLOSURES		P	S		O			
PM-23	DATA QUALITY MANAGEMENT		P	R	A	O			
PM-23(1)	AUTOMATION		P	D	A	O			
PM-23(2)	DATA TAGGING		P	D	A	O			
PM-23(3)	UPDATING PERSONALLY IDENTIFIABLE INFORMATION		P	S	A	O			
PM-24	DATA MANAGEMENT BOARD		P	S	A	O			
PM-25	DATA INTEGRITY BOARD		P	S	A	O			
PM-25(1)	PUBLISH AGREEMENTS ON WEBSITE		P			O			
PM-26	MINIMIZATION OF PII USED IN TESTING TRAINING, AND RESEARCH		P	S		O			
PM-27	INDIVIDUAL ACCESS CONTROL		P	S		O			
PM-28	COMPLAINT MANAGEMENT		P	S		O			
PM-29	INVENTORY OF PII		P	R		O			
PM-29(1)	AUTOMATION SUPPORT		P			O			
PM-30	PRIVACY REPORTING		P	R		O			
PM-31	SUPPLY CHAIN RISK MANAGEMENT PLAN					O			
PM-32	RISK FRAMING		P		A	O			

PERSONNEL SECURITY (PS)

PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES				A	O	x	x	x
PS-2	POSITION RISK DESIGNATION					O	x	x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
PS-3	PERSONNEL SCREENING					O	x	x	x
PS-3(1)	CLASSIFIED INFORMATION					O			
PS-3(2)	FORMAL INDOCTRINATION					O			
PS-3(3)	INFORMATION WITH SPECIAL PROTECTION MEASURES					O			
PS-3(4)	CITIZENSHIP REQUIREMENTS					O			
PS-4	PERSONNEL TERMINATION					O	x	x	x
PS-4(1)	POST-EMPLOYMENT REQUIREMENTS					O			
PS-4(2)	AUTOMATED NOTIFICATION					O			x
PS-5	PERSONNEL TRANSFER					O	x	x	x
PS-6	ACCESS AGREEMENTS				A	O	x	x	x
PS-6(1)	INFORMATION REQUIRING SPECIAL PROTECTION	W		Incorporated into PS-3.					
PS-6(2)	CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION				A	O			
PS-6(3)	POST-EMPLOYMENT REQUIREMENTS				A	O			
PS-7	EXTERNAL PERSONNEL SECURITY				A	O	x	x	x
PS-8	PERSONNEL SANCTIONS					O	x	x	x
RISK ASSESSMENT (RA)									
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES			R	A	O	x	x	x
RA-2	SECURITY CATEGORIZATION					O	x	x	x
RA-2(1)	SECOND-LEVEL CATEGORIZATION					O			
RA-3	RISK ASSESSMENT			S	A	O	x	x	x
RA-3(1)	SUPPLY CHAIN RISK ASSESSMENT					O		x	x
RA-4	RISK ASSESSMENT UPDATE	W		Incorporated into RA-3.					
RA-5	VULNERABILITY SCANNING				A	O	x	x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
RA-5(1)	UPDATE TOOL CAPABILITY	W	Incorporated into RA-5.						
RA-5(2)	UPDATE BY FREQUENCY, PRIOR TO NEW SCAN, OR WHEN IDENTIFIED				A	O	x	x	x
RA-5(3)	BREADTH AND DEPTH OF COVERAGE				A	O			
RA-5(4)	DISCOVERABLE INFORMATION				A	O			x
RA-5(5)	PRIVILEGED ACCESS				A	O		x	x
RA-5(6)	AUTOMATED TREND ANALYSES				A	O			
RA-5(7)	AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS	W	Incorporated into CM-8.						
RA-5(8)	REVIEW HISTORIC AUDIT LOGS				A	O			
RA-5(9)	PENETRATION TESTING AND ANALYSES	W	Incorporated into CA-8.						
RA-5(10)	CORRELATE SCANNING INFORMATION				A	O			
RA-6	TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY				A	O			
RA-7	RISK RESPONSE			S	A	O	x	x	x
RA-8	PRIVACY IMPACT ASSESSMENTS			S	A	O			
RA-9	CRITICALITY ANALYSIS					O		x	x
SYSTEM AND SERVICES ACQUISITION (SA)									
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES		P	R	A	O	x	x	x
SA-2	ALLOCATION OF RESOURCES				A	O	x	x	x
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE		P	D	A	O	x	x	x
SA-3(1)	MANAGE DEVELOPMENT ENVIRONMENT				A	O			
SA-3(2)	USE OF LIVE DATA				A	O			
SA-3(3)	TECHNOLOGY REFRESH				A	O			
SA-4	ACQUISITION PROCESS		P	R	A	O	x	x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SA-4(1)	FUNCTIONAL PROPERTIES OF CONTROLS				A	O		x	x
SA-4(2)	DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS				A	O		x	x
SA-4(3)	DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES				A	O			
SA-4(4)	ASSIGNMENT OF COMPONENTS TO SYSTEMS	W	Incorporated into CM-8(9).						
SA-4(5)	SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS				A	O			x
SA-4(6)	USE OF INFORMATION ASSURANCE PRODUCTS				A	O			
SA-4(7)	NIAP-APPROVED PROTECTION PROFILES				A	O			
SA-4(8)	CONTINUOUS MONITORING PLAN FOR CONTROLS				A	O			
SA-4(9)	FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE				A	O		x	x
SA-4(10)	USE OF APPROVED PIV PRODUCTS				A	O	x	x	x
SA-5	SYSTEM DOCUMENTATION				A	O	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).						
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		P	D	A	O	x	x	x
SA-9	EXTERNAL SYSTEM SERVICES		P	S	A	O	x	x	x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SA-9(1)	RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS				A	O			
SA-9(2)	IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES				A	O		x	x
SA-9(3)	ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS		P	D	A	O			
SA-9(4)	CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS				A	O			
SA-9(5)	PROCESSING, STORAGE, AND SERVICE LOCATION		P	D	A	O			
SA-9(6)	ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS				A	O			
SA-9(7)	ORGANIZATION-CONTROLLED INTEGRITY CHECKING				A	O			
SA-10	DEVELOPER CONFIGURATION MANAGEMENT				A	O		x	x
SA-10(1)	SOFTWARE AND FIRMWARE INTEGRITY VERIFICATION				A	O			
SA-10(2)	ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES				A	O			
SA-10(3)	HARDWARE INTEGRITY VERIFICATION				A	O			
SA-10(4)	TRUSTED GENERATION				A	O			
SA-10(5)	MAPPING INTEGRITY FOR VERSION CONTROL				A	O			
SA-10(6)	TRUSTED DISTRIBUTION				A	O			
SA-11	DEVELOPER TESTING AND EVALUATION		P	S	A	O		x	x
SA-11(1)	STATIC CODE ANALYSIS				A	O			
SA-11(2)	THREAT MODELING AND VULNERABILITY ANALYSES				A	O			
SA-11(3)	INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE				A	O			
SA-11(4)	MANUAL CODE REVIEWS				A	O			
SA-11(5)	PENETRATION TESTING				A	O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SA-11(6)	ATTACK SURFACE REVIEWS				A	O			
SA-11(7)	VERIFY SCOPE OF TESTING AND EVALUATION				A	O			
SA-11(8)	DYNAMIC CODE ANALYSIS				A	O			
SA-12	SUPPLY CHAIN RISK MANAGEMENT				A	O		x	x
SA-12(1)	ACQUISITION STRATEGIES, TOOLS, AND METHODS				A	O			
SA-12(2)	SUPPLIER REVIEWS				A	O			
SA-12(3)	TRUSTED SHIPPING AND WAREHOUSING	W	Incorporated into SA-12(1).						
SA-12(4)	DIVERSITY OF SUPPLIERS	W	Incorporated into SA-12(13).						
SA-12(5)	LIMITATION OF HARM				A	O			
SA-12(6)	MINIMIZING PROCUREMENT TIME	W	Incorporated into SA-12(1).						
SA-12(7)	ASSESSMENTS PRIOR TO SELECTION, ACCEPTANCE, AND UPDATE				A	O			
SA-12(8)	USE OF ALL-SOURCE INTELLIGENCE				A	O			
SA-12(9)	OPERATIONS SECURITY				A	O			
SA-12(10)	VALIDATE AS GENUINE AND NOT ALTERED				A	O			
SA-12(11)	PENETRATION TESTING AND ANALYSIS				A	O			
SA-12(12)	NOTIFICATION AGREEMENTS				A	O			
SA-12(13)	CRITICAL SYSTEM COMPONENTS	W	Incorporated into MA-6 and RA-9.						
SA-12(14)	IDENTITY AND TRACEABILITY				A	O			
SA-12(15)	PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES				A	O			
SA-12(16)	PROVENANCE				A	O			
SA-13	TRUSTWORTHINESS	W	Incorporated into SA-8.						
SA-14	CRITICALITY ANALYSIS	W	Incorporated into RA-9.						

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SA-14(1)	CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING	W	Incorporated into SA-20.						
SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS				A	O		x	x
SA-15(1)	QUALITY METRICS				A	O			
SA-15(2)	SECURITY TRACKING TOOLS				A	O			
SA-15(3)	CRITICALITY ANALYSIS				A	O		x	x
SA-15(4)	THREAT MODELING AND VULNERABILITY ANALYSIS	W	Incorporated into SA-11(2).						
SA-15(5)	ATTACK SURFACE REDUCTION				A	O			
SA-15(6)	CONTINUOUS IMPROVEMENT				A	O			
SA-15(7)	AUTOMATED VULNERABILITY ANALYSIS				A	O			
SA-15(8)	REUSE OF THREAT AND VULNERABILITY INFORMATION				A	O			
SA-15(9)	USE OF LIVE DATA	W	Incorporated into SA-3(2).						
SA-15(10)	INCIDENT RESPONSE PLAN				A	O			
SA-15(11)	ARCHIVE SYSTEM OR COMPONENT				A	O			
SA-16	DEVELOPER-PROVIDED TRAINING				A	O			x
SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN				A	O			x
SA-17(1)	FORMAL POLICY MODEL				A	O			
SA-17(2)	SECURITY-RELEVANT COMPONENTS				A	O			
SA-17(3)	FORMAL CORRESPONDENCE				A	O			
SA-17(4)	INFORMAL CORRESPONDENCE				A	O			
SA-17(5)	CONCEPTUALLY SIMPLE DESIGN				A	O			
SA-17(6)	STRUCTURE FOR TESTING				A	O			
SA-17(7)	STRUCTURE FOR LEAST PRIVILEGE				A	O			
SA-18	TAMPER RESISTANCE AND DETECTION				A	O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SA-18(1)	MULTIPLE PHASES OF SYSTEM DEVELOPMENT LIFE CYCLE				A	O			
SA-18(2)	INSPECTION OF SYSTEMS OR COMPONENTS				A	O			
SA-19	COMPONENT AUTHENTICITY				A	O			
SA-19(1)	ANTI-COUNTERFEIT TRAINING				A	O			
SA-19(2)	CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR				A	O			
SA-19(3)	COMPONENT DISPOSAL				A	O			
SA-19(4)	ANTI-COUNTERFEIT SCANNING				A	O			
SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS				A	O			
SA-21	DEVELOPER SCREENING				A	O			x
SA-21(1)	VALIDATION OF SCREENING	W	Incorporated into SA-21.						
SA-22	UNSUPPORTED SYSTEM COMPONENTS				A	O	x	x	x
SA-22(1)	ALTERNATIVE SOURCES FOR CONTINUED SUPPORT				A	O			

SYSTEM AND COMMUNICATIONS (SC)

SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES		P	R	A	O	x	x	x
SC-2	APPLICATION PARTITIONING				A	S		x	x
SC-2(1)	INTERFACES FOR NON-PRIVILEGED USERS				A	S			
SC-3	SECURITY FUNCTION ISOLATION				A	S			x
SC-3(1)	HARDWARE SEPARATION				A	S			
SC-3(2)	ACCESS AND FLOW CONTROL FUNCTIONS				A	S			
SC-3(3)	MINIMIZE NONSECURITY FUNCTIONALITY				A	O/S			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SC-3(4)	MODULE COUPLING AND COHESIVENESS				A	O/S			
SC-3(5)	LAYERED STRUCTURES				A	O/S			
SC-4	INFORMATION IN SHARED SYSTEM RESOURCES					S		x	x
SC-4(1)	SECURITY LEVELS	W		Incorporated into SC-4.					
SC-4(2)	MULTILEVEL OR PERIODS PROCESSING					S			
SC-5	DENIAL OF SERVICE PROTECTION					S	x	x	x
SC-5(1)	RESTRICT INTERNAL USERS					S			
SC-5(2)	CAPACITY, BANDWIDTH, AND REDUNDANCY					S			
SC-5(3)	DETECTION AND MONITORING					S			
SC-6	RESOURCE AVAILABILITY				A	S			
SC-7	BOUNDARY PROTECTION					S	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					S		x	x
SC-7(4)	EXTERNAL TELECOMMUNICATIONS SERVICES					O		x	x
SC-7(5)	DENY BY DEFAULT — ALLOW BY EXCEPTION					S		x	x
SC-7(6)	RESPONSE TO RECOGNIZED FAILURES	W		Incorporated into SC-7(18).					
SC-7(7)	PREVENT SPLIT TUNNELING FOR REMOTE DEVICES					S		x	x
SC-7(8)	ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS					S		x	x
SC-7(9)	RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC					S			
SC-7(10)	PREVENT EXFILTRATION					S			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
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)	PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS					S			
SC-7(15)	ROUTE PRIVILEGED NETWORK ACCESSES					S			
SC-7(16)	PREVENT DISCOVERY OF COMPONENTS AND DEVICES					S			
SC-7(17)	AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS					S			
SC-7(18)	FAIL SECURE				A	S			x
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				A	O/S			x
SC-7(22)	SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS				A	S			
SC-7(23)	DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE					S			
SC-7(24)	PERSONALLY IDENTIFIABLE INFORMATION		P	D		O/S			
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY					S		x	x
SC-8(1)	CRYPTOGRAPHIC PROTECTION					S		x	x
SC-8(2)	PRE- AND POST-TRANSMISSION HANDLING					S			
SC-8(3)	CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS					S			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SC-8(4)	CONCEAL OR RANDOMIZE COMMUNICATIONS					S			
SC-9	TRANSMISSION CONFIDENTIALITY	W	Incorporated into SC-8.						
SC-10	NETWORK DISCONNECT					S		x	x
SC-11	TRUSTED PATH				A	S			
SC-11(1)	LOGICAL ISOLATION				A	S			
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT					O/S	x	x	x
SC-12(1)	AVAILABILITY					O/S			x
SC-12(2)	SYMMETRIC KEYS					O/S			
SC-12(3)	ASYMMETRIC KEYS					O/S			
SC-12(4)	PKI CERTIFICATES	W	Incorporated into SC-12.						
SC-12(5)	PKI CERTIFICATES / HARDWARE TOKENS	W	Incorporated into SC-12.						
SC-13	CRYPTOGRAPHIC PROTECTION					S	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, SI-3, SI-4, SI-5, SI-7, SI-10.						
SC-15	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS					S	x	x	x
SC-15(1)	PHYSICAL DISCONNECT					S			
SC-15(2)	BLOCKING INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	W	Incorporated into SC-7.						
SC-15(3)	DISABLING AND REMOVAL IN SECURE WORK AREAS					O			
SC-15(4)	EXPLICITLY INDICATE CURRENT PARTICIPANTS					S			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SC-16	TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES		P	D		S			
SC-16(1)	INTEGRITY VALIDATION					S			
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES					O/S		x	x
SC-18	MOBILE CODE					O		x	x
SC-18(1)	IDENTIFY UNACCEPTABLE CODE AND TAKE CORRECTIVE ACTIONS					S			
SC-18(2)	ACQUISITION, DEVELOPMENT, AND USE					O			
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					O		x	x
SC-20	SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)					S	x	x	x
SC-20(1)	CHILD SUBSPACES	W	Incorporated into SC-20.						
SC-20(2)	DATA ORIGIN AND INTEGRITY					S			
SC-21	SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)					S	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					S	x	x	x
SC-23	SESSION AUTHENTICITY					S		x	x
SC-23(1)	INVALIDATE SESSION IDENTIFIERS AT LOGOUT					S			
SC-23(2)	USER-INITIATED LOGOUTS AND MESSAGE DISPLAYS	W	Incorporated into AC-12(1).						
SC-23(3)	UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION					S			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SC-23(4)	UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION	W	Incorporated into SC-23(3).						
SC-23(5)	ALLOWED CERTIFICATE AUTHORITIES					S			
SC-24	FAIL IN KNOWN STATE				A	S			x
SC-25	THIN NODES					S			
SC-26	HONEYPOTS					S			
SC-26(1)	DETECTION OF MALICIOUS CODE	W	Incorporated into SC-35.						
SC-27	PLATFORM-INDEPENDENT APPLICATIONS					S			
SC-28	PROTECTION OF INFORMATION AT REST					S		x	x
SC-28(1)	CRYPTOGRAPHIC PROTECTION					S		x	x
SC-28(2)	OFF-LINE STORAGE					O			
SC-29	HETEROGENEITY				A	O			
SC-29(1)	VIRTUALIZATION TECHNIQUES				A	O			
SC-30	CONCEALMENT AND MISDIRECTION				A	O			
SC-30(1)	VIRTUALIZATION TECHNIQUES	W	Incorporated into SC-29(1).						
SC-30(2)	RANDOMNESS				A	O			
SC-30(3)	CHANGE PROCESSING AND STORAGE LOCATIONS				A	O			
SC-30(4)	MISLEADING INFORMATION				A	O			
SC-30(5)	CONCEALMENT OF SYSTEM COMPONENTS				A	O			
SC-31	COVERT CHANNEL ANALYSIS				A	O			
SC-31(1)	TEST COVERT CHANNELS FOR EXPLOITABILITY				A	O			
SC-31(2)	MAXIMUM BANDWIDTH				A	O			
SC-31(3)	MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS				A	O			
SC-32	SYSTEM PARTITIONING				A	O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SC-33	TRANSMISSION PREPARATION INTEGRITY	W		Incorporated into SC-8.					
SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS				A	S			
SC-34(1)	NO WRITABLE STORAGE				A	O			
SC-34(2)	INTEGRITY PROTECTION AND READ-ONLY MEDIA				A	O			
SC-34(3)	HARDWARE-BASED PROTECTION				A	O			
SC-35	HONEYCLIENTS					S			
SC-36	DISTRIBUTED PROCESSING AND STORAGE				A	O			
SC-36(1)	POLLING TECHNIQUES				A	O			
SC-37	OUT-OF-BAND CHANNELS				A	O			
SC-37(1)	ENSURE DELIVERY AND TRANSMISSION				A	O			
SC-38	OPERATIONS SECURITY				A	O			
SC-39	PROCESS ISOLATION				A	S	x	x	x
SC-39(1)	HARDWARE SEPARATION				A	S			
SC-39(2)	THREAD ISOLATION				A	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					O			
SC-42	SENSOR CAPABILITY AND DATA					S			
SC-42(1)	REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES					O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SC-42(2)	AUTHORIZED USE		P	D		O			
SC-42(3)	PROHIBIT USE OF DEVICES					O			
SC-42(4)	NOTICE OF COLLECTION		P	D		O			
SC-42(5)	COLLECTION MINIMIZATION		P	D		O			
SC-43	USAGE RESTRICTIONS					O/S			
SC-44	DETONATION CHAMBERS					O			
SYSTEM AND INFORMATION INTEGRITY (SI)									
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES		P	D	A	O	x	x	x
SI-2	FLAW REMEDIATION					O	x	x	x
SI-2(1)	CENTRAL MANAGEMENT					O			x
SI-2(2)	AUTOMATED FLAW REMEDIATION STATUS					O		x	x
SI-2(3)	TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS					O			
SI-2(4)	AUTOMATED PATCH MANAGEMENT TOOLS	W	Incorporated into SI-2.						
SI-2(5)	AUTOMATIC SOFTWARE AND FIRMWARE UPDATES					O			
SI-2(6)	REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE AND FIRMWARE					O			
SI-2(7)	PERSONALLY IDENTIFIABLE INFORMATION		P	D		O			
SI-3	MALICIOUS CODE PROTECTION					O	x	x	x
SI-3(1)	CENTRAL MANAGEMENT					O		x	x
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					O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SI-3(5)	PORTABLE STORAGE DEVICES	W	Incorporated into MP-7.						
SI-3(6)	TESTING AND VERIFICATION					O			
SI-3(7)	NONSIGNATURE-BASED DETECTION	W	Incorporated into SI-3.						
SI-3(8)	DETECT UNAUTHORIZED COMMANDS					S			
SI-3(9)	AUTHENTICATE REMOTE COMMANDS					S			
SI-3(10)	MALICIOUS CODE ANALYSIS					O			
SI-4	SYSTEM MONITORING				A	O/S	x	x	x
SI-4(1)	SYSTEM-WIDE INTRUSION DETECTION SYSTEM				A	O/S			
SI-4(2)	AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS				A	S		x	x
SI-4(3)	AUTOMATED TOOL AND MECHANISM INTEGRATION				A	S			
SI-4(4)	INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC				A	S		x	x
SI-4(5)	SYSTEM-GENERATED ALERTS				A	S		x	x
SI-4(6)	RESTRICT NON-PRIVILEGED USERS	W	Incorporated into AC-6(10).						
SI-4(7)	AUTOMATED RESPONSE TO SUSPICIOUS EVENTS				A	S			
SI-4(8)	PROTECTION OF MONITORING INFORMATION	W	Incorporated into SI-4.						
SI-4(9)	TESTING OF MONITORING TOOLS AND MECHANISMS				A	O			
SI-4(10)	VISIBILITY OF ENCRYPTED COMMUNICATIONS				A	O			x
SI-4(11)	ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES				A	O/S			
SI-4(12)	AUTOMATED ORGANIZATION-GENERATED ALERTS				A	O/S			x
SI-4(13)	ANALYZE TRAFFIC AND EVENT PATTERNS				A	O/S			
SI-4(14)	WIRELESS INTRUSION DETECTION				A	S			x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SI-4(15)	WIRELESS TO WIRELINE COMMUNICATIONS				A	S			
SI-4(16)	CORRELATE MONITORING INFORMATION				A	O/S			
SI-4(17)	INTEGRATED SITUATIONAL AWARENESS				A	O			
SI-4(18)	ANALYZE TRAFFIC AND COVERT EXFILTRATION				A	O/S			
SI-4(19)	INDIVIDUALS POSING GREATER RISK				A	O			
SI-4(20)	PRIVILEGED USERS				A	S			x
SI-4(21)	PROBATIONARY PERIODS				A	O			
SI-4(22)	UNAUTHORIZED NETWORK SERVICES				A	S			x
SI-4(23)	HOST-BASED DEVICES				A	O			
SI-4(24)	INDICATORS OF COMPROMISE				A	S			
SI-4(25)	PERSONALLY IDENTIFIABLE INFORMATION MONITORING		P	D	A	O/S			
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES				A	O	x	x	x
SI-5(1)	AUTOMATED ALERTS AND ADVISORIES				A	O			x
SI-6	SECURITY AND PRIVACY FUNCTION VERIFICATION		P	D	A	S			x
SI-6(1)	NOTIFICATION OF FAILED SECURITY TESTS	W		Incorporated into SI-6.					
SI-6(2)	AUTOMATION SUPPORT FOR DISTRIBUTED TESTING					S			
SI-6(3)	REPORT VERIFICATION RESULTS		P	D		O			
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY				A	O/S		x	x
SI-7(1)	INTEGRITY CHECKS				A	S		x	x
SI-7(2)	AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS				A	S			x

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SI-7(3)	CENTRALLY MANAGED INTEGRITY TOOLS				A	O			
SI-7(4)	TAMPER-EVIDENT PACKAGING	W		Incorporated into SA-12.					
SI-7(5)	AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS				A	S			x
SI-7(6)	CRYPTOGRAPHIC PROTECTION				A	S			
SI-7(7)	INTEGRATION OF DETECTION AND RESPONSE				A	O		x	x
SI-7(8)	AUDITING CAPABILITY FOR SIGNIFICANT EVENTS				A	S			
SI-7(9)	VERIFY BOOT PROCESS				A	S			
SI-7(10)	PROTECTION OF BOOT FIRMWARE				A	S			
SI-7(11)	CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES				A	O			
SI-7(12)	INTEGRITY VERIFICATION				A	O/S			
SI-7(13)	CODE EXECUTION IN PROTECTED ENVIRONMENTS				A	O/S			
SI-7(14)	BINARY OR MACHINE EXECUTABLE CODE				A	O/S			x
SI-7(15)	CODE AUTHENTICATION				A	S			x
SI-7(16)	TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION				A	O			
SI-8	SPAM PROTECTION					O		x	x
SI-8(1)	CENTRAL MANAGEMENT					O		x	x
SI-8(2)	AUTOMATIC UPDATES					S		x	x
SI-8(3)	CONTINUOUS LEARNING CAPABILITY					S			
SI-9	INFORMATION INPUT RESTRICTIONS	W		Incorporated into AC-2, AC-3, AC-5, AC-6.					
SI-10	INFORMATION INPUT VALIDATION				A	S		x	x
SI-10(1)	MANUAL OVERRIDE CAPABILITY				A	O/S			
SI-10(2)	REVIEW AND RESOLVE OF ERRORS				A	O			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SI-10(3)	PREDICTABLE BEHAVIOR				A	O			
SI-10(4)	TIMING INTERACTIONS				A	S			
SI-10(5)	RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS				A	S			
SI-11	ERROR HANDLING					S		x	x
SI-12	INFORMATION MANAGEMENT AND RETENTION		P	R		O	x	x	x
SI-12(1)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS IN TESTING, TRAINING, AND RESEARCH		P	R		O			
SI-12(2)	MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION		P	R		O			
SI-13	PREDICTABLE FAILURE PREVENTION				A	O			
SI-13(1)	TRANSFERRING COMPONENT RESPONSIBILITIES				A	O			
SI-13(2)	TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION	W	Incorporated into SI-7(16).						
SI-13(3)	MANUAL TRANSFER BETWEEN COMPONENTS				A	O			
SI-13(4)	STANDBY COMPONENT INSTALLATION AND NOTIFICATION				A	O			
SI-13(5)	FAILOVER CAPABILITY				A	O			
SI-14	NON-PERSISTENCE				A	O			
SI-14(1)	REFRESH FROM TRUSTED SOURCES				A	O			
SI-15	INFORMATION OUTPUT FILTERING				A	S			
SI-15(1)	LIMIT PERSONALLY IDENTIFIABLE INFORMATION DISSEMINATION		P	S	A	O/S			
SI-16	MEMORY PROTECTION				A	S		x	x
SI-17	FAIL-SAFE PROCEDURES				A	S			
SI-18	INFORMATION DISPOSAL		P	D		O/S			
SI-19	DATA QUALITY OPERATIONS		P	D		O/S			

Control Number	Control Name (Control Enhancement Name)	Withdrawn	Privacy-Related	Selection Criteria	Assurance	Implemented By	Control Baseline Low	Control Baseline Mod	Control Baseline High
SI-19(1)	UPDATING AND CORRECTING PERSONALLY IDENTIFIABLE INFORMATION		P	S		O/S			
SI-19(2)	DATA TAGS		P	D		O/S			
SI-19(3)	PERSONALLY IDENTIFIABLE INFORMATION COLLECTION		P	S		O/S			
SI-20	DE-IDENTIFICATION		P	S		O/S			
SI-20(1)	COLLECTION		P	D		O/S			
SI-20(2)	ARCHIVING		P	D		O/S			
SI-20(3)	RELEASE		P	D		O/S			
SI-20(4)	REMOVAL, MASKING, ENCRYPTION, HASHING, OR REPLACEMENT OF DIRECT IDENTIFIERS		P	D		S			
SI-20(5)	STATISTICAL DISCLOSURE CONTROL		P	D		O/S			
SI-20(6)	DIFFERENTIAL PRIVACY		P	D		O/S			
SI-20(7)	VALIDATED SOFTWARE		P	D		O			
SI-20(8)	MOTIVATED INTRUDER		P	D		O/S			

Legend for NIST SP 800-53, Rev. 5, Security Control Guide

Privacy-Related Controls (fourth column)

Privacy-related controls are indicated by P in the fourth column.

Selection Criteria (fifth column)

Selection Criteria (fifth column) provides guidance to federal privacy programs in the selection of controls through three selection criteria tags: required (R), situationally required (S), and discretionary (D).

- R: Controls or control enhancements that are marked required must be selected and implemented based on applicable legal, regulatory, or policy requirements. Nonfederal organizations may use overlays to tailor their control selection to the laws, regulations, or policies applicable to their organizations.
- S: Privacy programs evaluate whether controls or control enhancements that are marked situationally required must be selected and implemented based on applicable legal, regulatory, or policy requirements, because these requirements only apply in specific circumstances. In the absence of any such requirements, the organization may treat these controls or enhancements as discretionary.
- D: Controls or control enhancements that are marked discretionary can be selected and implemented on an optional basis. Organizations use privacy risk assessments to inform and guide the selection and implementation of these controls or control enhancements to mitigate identified privacy risks.

Assurance (sixth column)

- A: Controls focused primarily on assurance. Assurance is the measure of confidence that the system functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system—thus possessing the capability to accurately mediate and enforce established security and privacy policies.

Implemented By (seventh column)

- S: A control or control enhancement that is typically implemented by an organizational system through technical means.
- O: A control or control enhancement that is typically implemented by an organization (i.e., by a human through nontechnical means).
- O/S: A control or control enhancement that can be implemented by an organization or a system or a combination of the two.

Control Baseline Allocation (eighth–tenth columns)

- A control or control enhancement that has been allocated to a control baseline is indicated by an “X” in the column for that baseline.
- A control or control enhancement that has not been allocated to a control baseline is indicated by a blank cell. Controls and control enhancements that are not allocated to any baseline can be selected on an optional basis.