

Control Sets for Cyber Security Fuel Cycle Facility Rulemaking

Notes:

- (1) Do not use this table without consulting the regulatory guide for specific guidance.
- (2) These controls reference controls from NIST SP 800-53, Revision 4.
- (3) For Set I and Set II control applicability to 3S systems, please refer to Facility Control Matrix
- (4) DBT control set denotes controls that apply only to security systems at Category I facilities

PROGRAM MANAGEMENT

Selected Program Management (PM) controls to be deployed organization-wide in support of the information security program. These controls are not associated with specific security control sets.

CNTL NO.	Control Name Control Enhancement Name	Control Selection
PM-1	Information Security Program Plan	X
PM-2	Senior Information Security Officer	X
PM-3	Information Security Resources	
PM-4	Plan of Action and Milestones Process	X
PM-5	Information System Inventory	
PM-6	Information Security Measures of Performance	X
PM-7	Enterprise Architecture	
PM-8	Critical Infrastructure Plan	
PM-9	Risk Management Strategy	X
PM-10	Security Authorization Process	X
PM-11	Mission/Business Process Definition	
PM-12	Insider Threat Program	X
PM-13	Information Security Workforce	X
PM-14	Testing, Training, and Monitoring	X
PM-15	Contacts with Security Groups and Associations	X
PM-16	Threat Awareness Program	X

ACCESS CONTROL

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
AC-1	Access Control Policy and Procedures	x	x	
AC-2	Account Management	x	x	
AC-2(1)	ACCOUNT MANAGEMENT / AUTOMATED SYSTEM ACCOUNT MANAGEMENT	x	x	
AC-2(2)	ACCOUNT MANAGEMENT / REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS	x	x	
AC-2(3)	ACCOUNT MANAGEMENT / DISABLE INACTIVE ACCOUNTS	x	x	
AC-2(4)	ACCOUNT MANAGEMENT / AUTOMATED AUDIT ACTIONS	x	x	
AC-2(5)	ACCOUNT MANAGEMENT / INACTIVITY LOGOUT		x	
AC-2(6)	ACCOUNT MANAGEMENT / DYNAMIC PRIVILEGE MANAGEMENT			
AC-2(7)	ACCOUNT MANAGEMENT / ROLE-BASED SCHEMES			
AC-2(8)	ACCOUNT MANAGEMENT / DYNAMIC ACCOUNT CREATION			
AC-2(9)	ACCOUNT MANAGEMENT / RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS			x
AC-2(10)	ACCOUNT MANAGEMENT / SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION			x
AC-2(11)	ACCOUNT MANAGEMENT / USAGE CONDITIONS		x	
AC-2(12)	ACCOUNT MANAGEMENT / ACCOUNT MONITORING / ATYPICAL USAGE		x	
AC-2(13)	ACCOUNT MANAGEMENT / DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS		x	
AC-3	Access Enforcement	x	x	
AC-3(2)	ACCESS ENFORCEMENT / DUAL AUTHORIZATION			x
AC-3(3)	ACCESS ENFORCEMENT / MANDATORY ACCESS CONTROL			
AC-3(4)	ACCESS ENFORCEMENT / DISCRETIONARY ACCESS CONTROL			
AC-3(5)	ACCESS ENFORCEMENT / SECURITY-RELEVANT INFORMATION			
AC-3(7)	ACCESS ENFORCEMENT / ROLE-BASED ACCESS CONTROL			
AC-3(8)	ACCESS ENFORCEMENT / REVOCATION OF ACCESS AUTHORIZATIONS			
AC-3(9)	ACCESS ENFORCEMENT / CONTROLLED RELEASE			
AC-3(10)	ACCESS ENFORCEMENT / AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS			
AC-4	Information Flow Enforcement	x	x	
AC-4(1)	INFORMATION FLOW ENFORCEMENT / OBJECT SECURITY ATTRIBUTES			
AC-4(2)	INFORMATION FLOW ENFORCEMENT / PROCESSING DOMAINS			
AC-4(3)	INFORMATION FLOW ENFORCEMENT / DYNAMIC INFORMATION FLOW CONTROL			
AC-4(4)	INFORMATION FLOW ENFORCEMENT / CONTENT CHECK ENCRYPTED INFORMATION			x
AC-4(5)	INFORMATION FLOW ENFORCEMENT / EMBEDDED DATA TYPES			
AC-4(6)	INFORMATION FLOW ENFORCEMENT / METADATA			
AC-4(7)	INFORMATION FLOW ENFORCEMENT / ONE-WAY FLOW MECHANISMS			
AC-4(8)	INFORMATION FLOW ENFORCEMENT / SECURITY POLICY FILTERS			
AC-4(9)	INFORMATION FLOW ENFORCEMENT / HUMAN REVIEWS			

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
AC-4(10)	INFORMATION FLOW ENFORCEMENT / ENABLE / DISABLE SECURITY POLICY FILTERS			
AC-4(11)	INFORMATION FLOW ENFORCEMENT / CONFIGURATION OF SECURITY POLICY FILTERS			
AC-4(12)	INFORMATION FLOW ENFORCEMENT / DATA TYPE IDENTIFIERS			
AC-4(13)	INFORMATION FLOW ENFORCEMENT / DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS			
AC-4(14)	INFORMATION FLOW ENFORCEMENT / SECURITY POLICY FILTER CONSTRAINTS			
AC-4(15)	INFORMATION FLOW ENFORCEMENT / DETECTION OF UNSANCTIONED INFORMATION			
AC-4(17)	INFORMATION FLOW ENFORCEMENT / DOMAIN AUTHENTICATION			
AC-4(18)	INFORMATION FLOW ENFORCEMENT / SECURITY ATTRIBUTE BINDING			
AC-4(19)	INFORMATION FLOW ENFORCEMENT / VALIDATION OF METADATA			
AC-4(20)	INFORMATION FLOW ENFORCEMENT / APPROVED SOLUTIONS			
AC-4(21)	INFORMATION FLOW ENFORCEMENT / PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS			X
AC-4(22)	INFORMATION FLOW ENFORCEMENT / ACCESS ONLY			
AC-5	Separation of Duties	X	X	
AC-6	Least Privilege	X	X	
AC-6(1)	LEAST PRIVILEGE / AUTHORIZE ACCESS TO SECURITY FUNCTIONS	X	X	
AC-6(2)	LEAST PRIVILEGE / NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	X	X	
AC-6(3)	LEAST PRIVILEGE / NETWORK ACCESS TO PRIVILEGED COMMANDS		X	
AC-6(4)	LEAST PRIVILEGE / SEPARATE PROCESSING DOMAINS			
AC-6(5)	LEAST PRIVILEGE / PRIVILEGED ACCOUNTS	X	X	
AC-6(6)	LEAST PRIVILEGE / PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS			
AC-6(7)	LEAST PRIVILEGE / REVIEW OF USER PRIVILEGES			
AC-6(8)	LEAST PRIVILEGE / PRIVILEGE LEVELS FOR CODE EXECUTION			
AC-6(9)	LEAST PRIVILEGE / AUDITING USE OF PRIVILEGED FUNCTIONS	X	X	
AC-6(10)	LEAST PRIVILEGE / PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	X	X	
AC-7	Unsuccessful Logon Attempts	X	X	
AC-7(2)	UNSUCCESSFUL LOGON ATTEMPTS / PURGE / WIPE MOBILE DEVICE			
AC-8	System Use Notification	X	X	
AC-9	Previous Logon (Access) Notification			
AC-9(1)	PREVIOUS LOGON NOTIFICATION / UNSUCCESSFUL LOGONS			X
AC-9(2)	PREVIOUS LOGON NOTIFICATION / SUCCESSFUL / UNSUCCESSFUL LOGONS			X
AC-9(3)	PREVIOUS LOGON NOTIFICATION / NOTIFICATION OF ACCOUNT CHANGES			X
AC-9(4)	PREVIOUS LOGON NOTIFICATION / ADDITIONAL LOGON INFORMATION			
AC-10	Concurrent Session Control		X	

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
AC-11	Session Lock	x	x	
AC-11(1)	SESSION LOCK / PATTERN-HIDING DISPLAYS	x	x	
AC-12	Session Termination	x	x	
AC-12(1)	SESSION TERMINATION / USER-INITIATED LOGOUTS / MESSAGE DISPLAYS			
AC-14	Permitted Actions without Identification or Authentication	x	x	
AC-16	Security Attributes			
AC-16(1)	SECURITY ATTRIBUTES / DYNAMIC ATTRIBUTE ASSOCIATION			
AC-16(2)	SECURITY ATTRIBUTES / ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS			
AC-16(3)	SECURITY ATTRIBUTES / MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM			
AC-16(4)	SECURITY ATTRIBUTES / ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS			x
AC-16(5)	SECURITY ATTRIBUTES / ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES			
AC-16(6)	SECURITY ATTRIBUTES / MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION			
AC-16(7)	SECURITY ATTRIBUTES / CONSISTENT ATTRIBUTE INTERPRETATION			
AC-16(8)	SECURITY ATTRIBUTES / ASSOCIATION TECHNIQUES / TECHNOLOGIES			
AC-16(9)	SECURITY ATTRIBUTES / ATTRIBUTE REASSIGNMENT			
AC-16(10)	SECURITY ATTRIBUTES / ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS			
AC-17	Remote Access	x	x	
AC-17(1)	REMOTE ACCESS / AUTOMATED MONITORING / CONTROL	x	x	
AC-17(2)	REMOTE ACCESS / PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION	x	x	
AC-17(3)	REMOTE ACCESS / MANAGED ACCESS CONTROL POINTS	x	x	
AC-17(4)	REMOTE ACCESS / PRIVILEGED COMMANDS / ACCESS	x	x	
AC-18	Wireless Access	x	x	
AC-18(1)	WIRELESS ACCESS / AUTHENTICATION AND ENCRYPTION	x	x	
AC-18(3)	WIRELESS ACCESS / DISABLE WIRELESS NETWORKING			
AC-18(4)	WIRELESS ACCESS / RESTRICT CONFIGURATIONS BY USERS		x	
AC-18(5)	WIRELESS ACCESS / ANTENNAS / TRANSMISSION POWER LEVELS		x	
AC-19	Access Control for Mobile Devices	x	x	
AC-19(4)	ACCESS CONTROL FOR MOBILE DEVICES / RESTRICTIONS FOR CLASSIFIED INFORMATION			
AC-19(5)	ACCESS CONTROL FOR MOBILE DEVICES / FULL DEVICE / CONTAINER-BASED ENCRYPTION	x	x	
AC-20	Use of External Information Systems	x	x	
AC-20(1)	USE OF EXTERNAL INFORMATION SYSTEMS / LIMITS ON AUTHORIZED USE	x	x	
AC-20(2)	USE OF EXTERNAL INFORMATION SYSTEMS / PORTABLE STORAGE DEVICES	x	x	

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
AC-20(3)	USE OF EXTERNAL INFORMATION SYSTEMS / NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES			X
AC-20(4)	USE OF EXTERNAL INFORMATION SYSTEMS / NETWORK ACCESSIBLE STORAGE DEVICES			X
AC-21	Information Sharing	X	X	
AC-21(1)	INFORMATION SHARING / AUTOMATED DECISION SUPPORT			
AC-21(2)	INFORMATION SHARING / INFORMATION SEARCH AND RETRIEVAL			
AC-22	Publicly Accessible Content	X	X	
AC-23	Data Mining Protection			
AC-24	Access Control Decisions			
AC-24(1)	ACCESS CONTROL DECISIONS / TRANSMIT ACCESS AUTHORIZATION INFORMATION			
AC-24(2)	ACCESS CONTROL DECISIONS / NO USER OR PROCESS IDENTITY			
AC-25	Reference Monitor			

AWARENESS AND TRAINING CONTROLS

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
AT-1	Security Awareness and Training Policy and Procedures	X	X	
AT-2	Security Awareness Training	X	X	
AT-2(1)	SECURITY AWARENESS / PRACTICAL EXERCISES			X
AT-2(2)	SECURITY AWARENESS / INSIDER THREAT		X	
AT-3	Role-Based Security Training	X	X	
AT-3(1)	ROLE-BASED SECURITY TRAINING / ENVIRONMENTAL CONTROLS			
AT-3(2)	ROLE-BASED SECURITY TRAINING / PHYSICAL SECURITY CONTROLS			
AT-3(3)	ROLE-BASED SECURITY TRAINING / PRACTICAL EXERCISES			X
AT-3(4)	ROLE-BASED SECURITY TRAINING / SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR			X
AT-4	Security Training Records	X	X	

AUDIT AND ACCOUNTABILITY CONTROLS

CNTL NO.	CONTROL NAME Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
AU-1	Audit and Accountability Policy and Procedures	X	X	
AU-2	Audit Events	X	X	
AU-2(3)	AUDIT EVENTS / REVIEWS AND UPDATES	X	X	
AU-3	Content of Audit Records	X	X	
AU-3(1)	CONTENT OF AUDIT RECORDS / ADDITIONAL AUDIT INFORMATION	X	X	
AU-3(2)	CONTENT OF AUDIT RECORDS / CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT		X	
AU-4	Audit Storage Capacity	X	X	
AU-4(1)	AUDIT STORAGE CAPACITY / TRANSFER TO ALTERNATE STORAGE			
AU-5	Response to Audit Processing Failures	X	X	
AU-5(1)	RESPONSE TO AUDIT PROCESSING FAILURES / AUDIT STORAGE CAPACITY		X	

CNTL NO.	CONTROL NAME Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
AU-5(2)	RESPONSE TO AUDIT PROCESSING FAILURES / REAL-TIME ALERTS		X	
AU-5(3)	RESPONSE TO AUDIT PROCESSING FAILURES / CONFIGURABLE TRAFFIC VOLUME THRESHOLDS			
AU-5(4)	RESPONSE TO AUDIT PROCESSING FAILURES / SHUTDOWN ON FAILURE			
AU-6	Audit Review, Analysis, and Reporting	X	X	
AU-6(1)	AUDIT REVIEW, ANALYSIS, AND REPORTING / PROCESS INTEGRATION	X	X	
AU-6(3)	AUDIT REVIEW, ANALYSIS, AND REPORTING / CORRELATE AUDIT REPOSITORIES	X	X	
AU-6(4)	AUDIT REVIEW, ANALYSIS, AND REPORTING / CENTRAL REVIEW AND ANALYSIS			
AU-6(5)	AUDIT REVIEW, ANALYSIS, AND REPORTING / INTEGRATION / SCANNING AND MONITORING CAPABILITIES		X	
AU-6(6)	AUDIT REVIEW, ANALYSIS, AND REPORTING / CORRELATION WITH PHYSICAL MONITORING		X	
AU-6(7)	AUDIT REVIEW, ANALYSIS, AND REPORTING / PERMITTED ACTIONS			X
AU-6(8)	AUDIT REVIEW, ANALYSIS, AND REPORTING / FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS			
AU-6(9)	AUDIT REVIEW, ANALYSIS, AND REPORTING / CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES			
AU-6(10)	AUDIT REVIEW, ANALYSIS, AND REPORTING / AUDIT LEVEL ADJUSTMENT			
AU-7	Audit Reduction and Report Generation	X	X	
AU-7(1)	AUDIT REDUCTION AND REPORT GENERATION / AUTOMATIC PROCESSING	X	X	
AU-7(2)	AUDIT REDUCTION AND REPORT GENERATION / AUTOMATIC SORT AND SEARCH			
AU-8	Time Stamps	X	X	
AU-8(1)	TIME STAMPS / SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	X	X	
AU-8(2)	TIME STAMPS / SECONDARY AUTHORITATIVE TIME SOURCE			
AU-9	Protection of Audit Information	X	X	
AU-9(1)	PROTECTION OF AUDIT INFORMATION / HARDWARE WRITE-ONCE MEDIA			
AU-9(2)	PROTECTION OF AUDIT INFORMATION / AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS		X	
AU-9(3)	PROTECTION OF AUDIT INFORMATION / CRYPTOGRAPHIC PROTECTION		X	
AU-9(4)	PROTECTION OF AUDIT INFORMATION / ACCESS BY SUBSET OF PRIVILEGED USERS	X	X	
AU-9(5)	PROTECTION OF AUDIT INFORMATION / DUAL AUTHORIZATION			X
AU-9(6)	PROTECTION OF AUDIT INFORMATION / READ-ONLY ACCESS			
AU-10	Non-repudiation		X	
AU-10(1)	NON-REPUDIATION / ASSOCIATION OF IDENTITIES			X
AU-10(2)	NON-REPUDIATION / VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY			X

CNTL NO.	CONTROL NAME Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
AU-10(3)	NON-REPUDIATION / CHAIN OF CUSTODY			X
AU-10(4)	NON-REPUDIATION / VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY			X
AU-11	Audit Record Retention	X	X	
AU-11(1)	AUDIT RECORD RETENTION / LONG-TERM RETRIEVAL CAPABILITY			
AU-12	Audit Generation	X	X	
AU-12(1)	AUDIT GENERATION / SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL		X	
AU-12(2)	AUDIT GENERATION / STANDARDIZED FORMATS			
AU-12(3)	AUDIT GENERATION / CHANGES BY AUTHORIZED INDIVIDUALS		X	
AU-13	Monitoring for Information Disclosure			
AU-13(1)	MONITORING FOR INFORMATION DISCLOSURE / USE OF AUTOMATED TOOLS			
AU-13(2)	MONITORING FOR INFORMATION DISCLOSURE / REVIEW OF MONITORED SITES			
AU-14	Session Audit			X
AU-14(1)	SESSION AUDIT / SYSTEM START-UP		X	
AU-14(2)	SESSION AUDIT / CAPTURE/RECORD AND LOG CONTENT		X	
AU-14(3)	SESSION AUDIT / REMOTE VIEWING / LISTENING			
AU-15	Alternate Audit Capability			
AU-16	Cross-Organizational Auditing			
AU-16(1)	CROSS-ORGANIZATIONAL AUDITING / IDENTITY PRESERVATION			
AU-16(2)	CROSS-ORGANIZATIONAL AUDITING / SHARING OF AUDIT INFORMATION			

SECURITY ASSESSMENT AND AUTHORIZATION CONTROLS

CNTL NO.	CONTROL NAME Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
CA-1	Security Assessment and Authorization Policies and Procedures	X	X	
CA-2	Security Assessments	X	X	
CA-2(1)	SECURITY ASSESSMENTS / INDEPENDENT ASSESSORS	X	X	
CA-2(2)	SECURITY ASSESSMENTS / SPECIALIZED ASSESSMENTS		X	
CA-2(3)	SECURITY ASSESSMENTS / EXTERNAL ORGANIZATIONS			
CA-3	System Interconnections	X	X	
CA-3(1)	SYSTEM INTERCONNECTIONS / UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS			X
CA-3(2)	SYSTEM INTERCONNECTIONS / CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS			X
CA-3(3)	SYSTEM INTERCONNECTIONS / UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS		X	
CA-3(4)	SYSTEM INTERCONNECTIONS / CONNECTIONS TO PUBLIC NETWORKS		X	
CA-3(5)	SYSTEM INTERCONNECTIONS / RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS	X	X	
CA-5	Plan of Action and Milestones	X	X	

CNTL NO.	CONTROL NAME Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
CA-5(1)	PLAN OF ACTION AND MILESTONES / AUTOMATION SUPPORT FOR ACCURACY / CURRENCY			
CA-6	Security Authorization	x	x	
CA-7	Continuous Monitoring	x	x	
CA-7(1)	CONTINUOUS MONITORING / INDEPENDENT ASSESSMENT	x	x	
CA-7(3)	CONTINUOUS MONITORING / TREND ANALYSES			
CA-8	Penetration Testing		x	
CA-8(1)	PENETRATION TESTING / INDEPENDENT PENETRATION AGENT OR TEAM	x	x	
CA-8(2)	PENETRATION TESTING / RED TEAM EXERCISES			x
CA-9	Internal System Connections	x	x	
CA-9(1)	INTERNAL SYSTEM CONNECTIONS / SECURITY COMPLIANCE CHECKS			x

CONFIGURATION MANAGEMENT CONTROLS

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
CM-1	Configuration Management Policy and Procedures	x	x	
CM-2	Baseline Configuration	x	x	
CM-2(1)	BASILINE CONFIGURATION / REVIEWS AND UPDATES	x	x	
CM-2(2)	BASILINE CONFIGURATION / AUTOMATION SUPPORT FOR ACCURACY / CURRENCY		x	
CM-2(3)	BASILINE CONFIGURATION / RETENTION OF PREVIOUS CONFIGURATIONS	x	x	
CM-2(6)	BASILINE CONFIGURATION / DEVELOPMENT AND TEST ENVIRONMENTS			
CM-2(7)	BASILINE CONFIGURATION / CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS	x	x	
CM-3	Configuration Change Control	x	x	
CM-3(1)	CONFIGURATION CHANGE CONTROL / AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES		x	
CM-3(2)	CONFIGURATION CHANGE CONTROL / TEST / VALIDATE / DOCUMENT CHANGES	x	x	
CM-3(3)	CONFIGURATION CHANGE CONTROL / AUTOMATED CHANGE IMPLEMENTATION			
CM-3(4)	CONFIGURATION CHANGE CONTROL / SECURITY REPRESENTATIVE			
CM-3(5)	CONFIGURATION CHANGE CONTROL / AUTOMATED SECURITY RESPONSE			
CM-3(6)	CONFIGURATION CHANGE CONTROL / CRYPTOGRAPHY MANAGEMENT			
CM-4	Security Impact Analysis	x	x	
CM-4(1)	SECURITY IMPACT ANALYSIS / SEPARATE TEST ENVIRONMENTS		x	
CM-4(2)	SECURITY IMPACT ANALYSIS / VERIFICATION OF SECURITY FUNCTIONS			x
CM-5	Access Restrictions for Change	x	x	

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
CM-5(1)	ACCESS RESTRICTIONS FOR CHANGE / AUTOMATED ACCESS ENFORCEMENT / AUDITING		X	
CM-5(2)	ACCESS RESTRICTIONS FOR CHANGE / REVIEW SYSTEM CHANGES		X	
CM-5(3)	ACCESS RESTRICTIONS FOR CHANGE / SIGNED COMPONENTS		X	
CM-5(4)	ACCESS RESTRICTIONS FOR CHANGE / DUAL AUTHORIZATION			X
CM-5(5)	ACCESS RESTRICTIONS FOR CHANGE / LIMIT PRODUCTION / OPERATIONAL PRIVILEGES			
CM-5(6)	ACCESS RESTRICTIONS FOR CHANGE / LIMIT LIBRARY PRIVILEGES			
CM-6	Configuration Settings	X	X	
CM-6(1)	CONFIGURATION SETTINGS / AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION		X	
CM-6(2)	CONFIGURATION SETTINGS / RESPOND TO UNAUTHORIZED CHANGES		X	
CM-7	Least Functionality	X	X	
CM-7(1)	LEAST FUNCTIONALITY / PERIODIC REVIEW	X	X	
CM-7(2)	LEAST FUNCTIONALITY / PREVENT PROGRAM EXECUTION	X	X	
CM-7(3)	LEAST FUNCTIONALITY / REGISTRATION COMPLIANCE			
CM-7(4)	LEAST FUNCTIONALITY / UNAUTHORIZED SOFTWARE / BLACKLISTING	X		
CM-7(5)	LEAST FUNCTIONALITY / AUTHORIZED SOFTWARE / WHITELISTING		X	
CM-8	Information System Component Inventory	X	X	
CM-8(1)	INFORMATION SYSTEM COMPONENT INVENTORY / UPDATES DURING INSTALLATIONS / REMOVALS	X	X	
CM-8(2)	INFORMATION SYSTEM COMPONENT INVENTORY / AUTOMATED MAINTENANCE		X	
CM-8(3)	INFORMATION SYSTEM COMPONENT INVENTORY / AUTOMATED UNAUTHORIZED COMPONENT DETECTION	X	X	
CM-8(4)	INFORMATION SYSTEM COMPONENT INVENTORY / ACCOUNTABILITY INFORMATION		X	
CM-8(5)	INFORMATION SYSTEM COMPONENT INVENTORY / NO DUPLICATE ACCOUNTING OF COMPONENTS	X	X	
CM-8(6)	INFORMATION SYSTEM COMPONENT INVENTORY / ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS			
CM-8(7)	INFORMATION SYSTEM COMPONENT INVENTORY / CENTRALIZED REPOSITORY			
CM-8(8)	INFORMATION SYSTEM COMPONENT INVENTORY / AUTOMATED LOCATION TRACKING			
CM-8(9)	INFORMATION SYSTEM COMPONENT INVENTORY / ASSIGNMENT OF COMPONENTS TO SYSTEMS			
CM-9	Configuration Management Plan	X	X	
CM-9(1)	CONFIGURATION MANAGEMENT PLAN / ASSIGNMENT OF RESPONSIBILITY			
CM-10	Software Usage Restrictions	X	X	
CM-10(1)	SOFTWARE USAGE RESTRICTIONS / OPEN SOURCE SOFTWARE			
CM-11	User-Installed Software	X	X	
CM-11(1)	USER-INSTALLED SOFTWARE / ALERTS FOR UNAUTHORIZED INSTALLATIONS			X

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
CM-11(2)	USER-INSTALLED SOFTWARE / PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS			X

CONTINGENCY PLANNING CONTROLS

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		SET II	SET I	DBT
CP-1	Contingency Planning Policy and Procedures	X	X	
CP-2	Contingency Plan	X	X	
CP-2(1)	CONTINGENCY PLAN / COORDINATE WITH RELATED PLANS	X	X	
CP-2(2)	CONTINGENCY PLAN / CAPACITY PLANNING		X	
CP-2(3)	CONTINGENCY PLAN / RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS	X	X	
CP-2(4)	CONTINGENCY PLAN / RESUME ALL MISSIONS / BUSINESS FUNCTIONS		X	
CP-2(5)	CONTINGENCY PLAN / CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS		X	
CP-2(6)	CONTINGENCY PLAN / ALTERNATE PROCESSING / STORAGE SITE			
CP-2(7)	CONTINGENCY PLAN / COORDINATE WITH EXTERNAL SERVICE PROVIDERS			
CP-2(8)	CONTINGENCY PLAN / IDENTIFY CRITICAL ASSETS	X	X	
CP-3	Contingency Training	X	X	
CP-3(1)	CONTINGENCY TRAINING / SIMULATED EVENTS		X	
CP-3(2)	CONTINGENCY TRAINING / AUTOMATED TRAINING ENVIRONMENTS			
CP-4	Contingency Plan Testing	X	X	
CP-4(1)	CONTINGENCY PLAN TESTING / COORDINATE WITH RELATED PLANS	X	X	
CP-4(2)	CONTINGENCY PLAN TESTING / ALTERNATE PROCESSING SITE		X	
CP-4(3)	CONTINGENCY PLAN TESTING / AUTOMATED TESTING			
CP-4(4)	CONTINGENCY PLAN TESTING / FULL RECOVERY / RECONSTITUTION			
CP-6	Alternate Storage Site	X	X	
CP-6(1)	ALTERNATE STORAGE SITE / SEPARATION FROM PRIMARY SITE	X	X	
CP-6(2)	ALTERNATE STORAGE SITE / RECOVERY TIME / POINT OBJECTIVES		X	
CP-6(3)	ALTERNATE STORAGE SITE / ACCESSIBILITY	X	X	
CP-7	Alternate Processing Site	X	X	
CP-7(1)	ALTERNATE PROCESSING SITE / SEPARATION FROM PRIMARY SITE	X	X	
CP-7(2)	ALTERNATE PROCESSING SITE / ACCESSIBILITY	X	X	
CP-7(3)	ALTERNATE PROCESSING SITE / PRIORITY OF SERVICE	X	X	
CP-7(4)	ALTERNATE PROCESSING SITE / PREPARATION FOR USE		X	
CP-7(6)	ALTERNATE PROCESSING SITE / INABILITY TO RETURN TO PRIMARY SITE			
CP-8	Telecommunications Services	X	X	

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		SET II	SET I	DBT
CP-8(1)	TELECOMMUNICATIONS SERVICES / PRIORITY OF SERVICE PROVISIONS	X	X	
CP-8(2)	TELECOMMUNICATIONS SERVICES / SINGLE POINTS OF FAILURE	X	X	
CP-8(3)	TELECOMMUNICATIONS SERVICES / SEPARATION OF PRIMARY / ALTERNATE PROVIDERS		X	
CP-8(4)	TELECOMMUNICATIONS SERVICES / PROVIDER CONTINGENCY PLAN		X	
CP-8(5)	TELECOMMUNICATIONS SERVICES / ALTERNATE TELECOMMUNICATION SERVICE TESTING			
CP-9	Information System Backup	X	X	
CP-9(1)	INFORMATION SYSTEM BACKUP / TESTING FOR RELIABILITY / INTEGRITY	X	X	
CP-9(2)	INFORMATION SYSTEM BACKUP / TEST RESTORATION USING SAMPLING		X	
CP-9(3)	INFORMATION SYSTEM BACKUP / SEPARATE STORAGE FOR CRITICAL INFORMATION		X	
CP-9(5)	INFORMATION SYSTEM BACKUP / TRANSFER TO ALTERNATE STORAGE SITE		X	
CP-9(6)	INFORMATION SYSTEM BACKUP / REDUNDANT SECONDARY SYSTEM			
CP-9(7)	INFORMATION SYSTEM BACKUP / DUAL AUTHORIZATION			X
CP-10	Information System Recovery and Reconstitution	X	X	
CP-10(2)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION / TRANSACTION RECOVERY	X	X	
CP-10(4)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION / RESTORE WITHIN TIME PERIOD		X	
CP-10(6)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION / COMPONENT PROTECTION			
CP-11	Alternate Communications Protocols			
CP-12	Safe Mode	X	X	

IDENTIFICATION AND AUTHENTICATION CONTROLS

CNTL NO.	CONTROL NAME Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
IA-1	Identification and Authentication Policy and Procedures	X	X	
IA-2	Identification and Authentication (Organizational Users)	X	X	
IA-2(1)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / NETWORK ACCESS TO PRIVILEGED ACCOUNTS	X	X	
IA-2(2)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS	X	X	
IA-2(3)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / LOCAL ACCESS TO PRIVILEGED ACCOUNTS	X	X	
IA-2(4)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS		X	
IA-2(5)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / GROUP AUTHENTICATION			

CNTL NO.	CONTROL NAME Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
IA-2(6)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE			
IA-2(7)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE			
IA-2(8)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT	X	X	
IA-2(9)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT		X	
IA-2(10)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / SINGLE SIGN-ON			
IA-2(11)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / REMOTE ACCESS - SEPARATE DEVICE	X	X	
IA-2(12)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) / ACCEPTANCE OF PIV CREDENTIALS	X	X	
IA-2(13)	IDENTIFICATION AND AUTHENTICATION / OUT-OF-BAND AUTHENTICATION			
IA-3	Device Identification and Authentication	X	X	
IA-3(1)	DEVICE IDENTIFICATION AND AUTHENTICATION / CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION			
IA-3(3)	DEVICE IDENTIFICATION AND AUTHENTICATION / DYNAMIC ADDRESS ALLOCATION			
IA-3(4)	DEVICE IDENTIFICATION AND AUTHENTICATION / DEVICE ATTESTATION			X
IA-4	Identifier Management	X	X	
IA-4(1)	IDENTIFIER MANAGEMENT / PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS			
IA-4(2)	IDENTIFIER MANAGEMENT / SUPERVISOR AUTHORIZATION			X
IA-4(3)	IDENTIFIER MANAGEMENT / MULTIPLE FORMS OF CERTIFICATION			
IA-4(4)	IDENTIFIER MANAGEMENT / IDENTIFY USER STATUS			
IA-4(5)	IDENTIFIER MANAGEMENT / DYNAMIC MANAGEMENT			
IA-4(6)	IDENTIFIER MANAGEMENT / CROSS-ORGANIZATION MANAGEMENT			
IA-4(7)	IDENTIFIER MANAGEMENT / IN-PERSON REGISTRATION			X
IA-5	Authenticator Management	X	X	
IA-5(1)	AUTHENTICATOR MANAGEMENT / PASSWORD-BASED AUTHENTICATION	X	X	
IA-5(2)	AUTHENTICATOR MANAGEMENT / PKI-BASED AUTHENTICATION	X	X	
IA-5(3)	AUTHENTICATOR MANAGEMENT / IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION	X	X	
IA-5(4)	AUTHENTICATOR MANAGEMENT / AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION			X
IA-5(5)	AUTHENTICATOR MANAGEMENT / CHANGE AUTHENTICATORS PRIOR TO DELIVERY			
IA-5(6)	AUTHENTICATOR MANAGEMENT / PROTECTION OF AUTHENTICATORS			

CNTL NO.	CONTROL NAME Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
IA-5(7)	AUTHENTICATOR MANAGEMENT / NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS			
IA-5(8)	AUTHENTICATOR MANAGEMENT / MULTIPLE INFORMATION SYSTEM ACCOUNTS			
IA-5(9)	AUTHENTICATOR MANAGEMENT / CROSS-ORGANIZATION CREDENTIAL MANAGEMENT			
IA-5(10)	AUTHENTICATOR MANAGEMENT / DYNAMIC CREDENTIAL ASSOCIATION			
IA-5(11)	AUTHENTICATOR MANAGEMENT / HARDWARE TOKEN-BASED AUTHENTICATION	x	x	
IA-5(12)	AUTHENTICATOR MANAGEMENT / BIOMETRIC-BASED AUTHENTICATION			
IA-5(13)	AUTHENTICATOR MANAGEMENT / EXPIRATION OF CACHED AUTHENTICATORS			
IA-5(14)	AUTHENTICATOR MANAGEMENT / MANAGING CONTENT OF PKI TRUST STORES			
IA-5(15)	AUTHENTICATOR MANAGEMENT / FICAM-APPROVED PRODUCTS AND SERVICES			
IA-6	Authenticator Feedback	x	x	
IA-7	Cryptographic Module Authentication	x	x	
IA-8	Identification and Authentication (Non-Organizational Users)	x	x	
IA-8(1)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) / ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES	x	x	
IA-8(2)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) / ACCEPTANCE OF THIRD-PARTY CREDENTIALS	x	x	
IA-8(3)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) / USE OF FICAM-APPROVED PRODUCTS	x	x	
IA-8(4)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) / USE OF FICAM-ISSUED PROFILES	x	x	
IA-8(5)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) / ACCEPTANCE OF PIV-I CREDENTIALS			
IA-9	Service Identification and Authentication			
IA-9(1)	SERVICE IDENTIFICATION AND AUTHENTICATION / INFORMATION EXCHANGE			
IA-9(2)	SERVICE IDENTIFICATION AND AUTHENTICATION / TRANSMISSION OF DECISIONS			
IA-10	Adaptive Identification and Authentication			
IA-11	Re-authentication			

INCIDENT RESPONSE CONTROLS

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
IR-1	Incident Response Policy and Procedures	x	x	
IR-2	Incident Response Training	x	x	
IR-2(1)	INCIDENT RESPONSE TRAINING / SIMULATED EVENTS		x	

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
IR-2(2)	INCIDENT RESPONSE TRAINING / AUTOMATED TRAINING ENVIRONMENTS		X	
IR-3	Incident Response Testing	X	X	
IR-3(1)	INCIDENT RESPONSE TESTING / AUTOMATED TESTING			
IR-3(2)	INCIDENT RESPONSE TESTING / COORDINATION WITH RELATED PLANS	X	X	
IR-4	Incident Handling	X	X	
IR-4(1)	INCIDENT HANDLING / AUTOMATED INCIDENT HANDLING PROCESSES	X	X	
IR-4(2)	INCIDENT HANDLING / DYNAMIC RECONFIGURATION			
IR-4(3)	INCIDENT HANDLING / CONTINUITY OF OPERATIONS			
IR-4(4)	INCIDENT HANDLING / INFORMATION CORRELATION		X	
IR-4(5)	INCIDENT HANDLING / AUTOMATIC DISABLING OF INFORMATION SYSTEM			
IR-4(6)	INCIDENT HANDLING / INSIDER THREATS - SPECIFIC CAPABILITIES			
IR-4(7)	INCIDENT HANDLING / INSIDER THREATS - INTRA-ORGANIZATION COORDINATION			
IR-4(8)	INCIDENT HANDLING / CORRELATION WITH EXTERNAL ORGANIZATIONS			
IR-4(9)	INCIDENT HANDLING / DYNAMIC RESPONSE CAPABILITY			
IR-4(10)	INCIDENT HANDLING / SUPPLY CHAIN COORDINATION			
IR-5	Incident Monitoring	X	X	
IR-5(1)	INCIDENT MONITORING / AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS		X	
IR-6	Incident Reporting	X	X	
IR-6(1)	INCIDENT REPORTING / AUTOMATED REPORTING	X	X	
IR-6(2)	INCIDENT REPORTING / VULNERABILITIES RELATED TO INCIDENTS			X
IR-6(3)	INCIDENT REPORTING / COORDINATION WITH SUPPLY CHAIN			
IR-7	Incident Response Assistance	X	X	
IR-7(1)	INCIDENT RESPONSE ASSISTANCE / AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT	X	X	
IR-7(2)	INCIDENT RESPONSE ASSISTANCE / COORDINATION WITH EXTERNAL PROVIDERS			
IR-8	Incident Response Plan	X	X	
IR-9	Information Spillage Response			X
IR-9(1)	INFORMATION SPILLAGE RESPONSE / RESPONSIBLE PERSONNEL			X
IR-9(2)	INFORMATION SPILLAGE RESPONSE / TRAINING			X
IR-9(3)	INFORMATION SPILLAGE RESPONSE / POST-SPILL OPERATIONS			X
IR-9(4)	INFORMATION SPILLAGE RESPONSE / EXPOSURE TO UNAUTHORIZED PERSONNEL			X
IR-10	Integrated Information Security Analysis Team		X	

MAINTENANCE CONTROLS

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
MA-1	System Maintenance Policy and Procedures	x	x	
MA-2	Controlled Maintenance	x	x	
MA-2(2)	CONTROLLED MAINTENANCE / AUTOMATED MAINTENANCE ACTIVITIES		x	
MA-3	Maintenance Tools	x	x	
MA-3(1)	MAINTENANCE TOOLS / INSPECT TOOLS	x	x	
MA-3(2)	MAINTENANCE TOOLS / INSPECT MEDIA	x	x	
MA-3(3)	MAINTENANCE TOOLS / PREVENT UNAUTHORIZED REMOVAL		x	
MA-3(4)	MAINTENANCE TOOLS / RESTRICTED TOOL USE			
MA-4	Nonlocal Maintenance	x	x	
MA-4(1)	NONLOCAL MAINTENANCE / AUDITING AND REVIEW			
MA-4(2)	NONLOCAL MAINTENANCE / DOCUMENT NONLOCAL MAINTENANCE	x	x	
MA-4(3)	NONLOCAL MAINTENANCE / COMPARABLE SECURITY / SANITIZATION		x	
MA-4(4)	NONLOCAL MAINTENANCE / AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS			
MA-4(5)	NONLOCAL MAINTENANCE / APPROVALS AND NOTIFICATIONS			
MA-4(6)	NONLOCAL MAINTENANCE / CRYPTOGRAPHIC PROTECTION			
MA-4(7)	NONLOCAL MAINTENANCE / REMOTE DISCONNECT VERIFICATION			
MA-5	Maintenance Personnel	x	x	
MA-5(1)	MAINTENANCE PERSONNEL / INDIVIDUALS WITHOUT APPROPRIATE ACCESS		x	
MA-5(2)	MAINTENANCE PERSONNEL / SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS			x
MA-5(3)	MAINTENANCE PERSONNEL / CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS		x	
MA-5(4)	MAINTENANCE PERSONNEL / FOREIGN NATIONALS			
MA-5(5)	MAINTENANCE PERSONNEL / NON-SYSTEM-RELATED MAINTENANCE			
MA-6	Timely Maintenance	x	x	
MA-6(1)	TIMELY MAINTENANCE / PREVENTIVE MAINTENANCE			
MA-6(2)	TIMELY MAINTENANCE / PREDICTIVE MAINTENANCE			
MA-6(3)	TIMELY MAINTENANCE / AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE			

MEDIA PROTECTION CONTROLS

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		SET II	SET I	DBT
MP-1	Media Protection Policy and Procedures	x	x	
MP-2	Media Access	x	x	
MP-3	Media Marking	x	x	
MP-4	Media Storage	x	x	
MP-4(2)	MEDIA STORAGE / AUTOMATED RESTRICTED ACCESS			
MP-5	Media Transport	x	x	
MP-5(3)	MEDIA TRANSPORT / CUSTODIANS			
MP-5(4)	MEDIA TRANSPORT / CRYPTOGRAPHIC PROTECTION	x	x	
MP-6	Media Sanitization	x	x	
MP-6(1)	MEDIA SANITIZATION / REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY		x	
MP-6(2)	MEDIA SANITIZATION / EQUIPMENT TESTING		x	
MP-6(3)	MEDIA SANITIZATION / NONDESTRUCTIVE TECHNIQUES		x	
MP-6(7)	MEDIA SANITIZATION / DUAL AUTHORIZATION			x
MP-6(8)	MEDIA SANITIZATION / REMOTE PURGING / WIPING OF INFORMATION			
MP-7	Media Use	x	x	
MP-7(1)	MEDIA USE / PROHIBIT USE WITHOUT OWNER	x	x	
MP-7(2)	MEDIA USE / PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA			x
MP-8	Media Downgrading			
MP-8(1)	MEDIA DOWNGRADING / DOCUMENTATION OF PROCESS			
MP-8(2)	MEDIA DOWNGRADING / EQUIPMENT TESTING			
MP-8(3)	MEDIA DOWNGRADING / CONTROLLED UNCLASSIFIED INFORMATION			
MP-8(4)	MEDIA DOWNGRADING / CLASSIFIED INFORMATION			

PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
PE-1	Physical and Environmental Protection Policy and Procedures	x	x	
PE-2	Physical Access Authorizations			
PE-2(1)	PHYSICAL ACCESS AUTHORIZATIONS / ACCESS BY POSITION / ROLE			
PE-2(2)	PHYSICAL ACCESS AUTHORIZATIONS / TWO FORMS OF IDENTIFICATION			
PE-2(3)	PHYSICAL ACCESS AUTHORIZATIONS / RESTRICT UNESCORTED ACCESS			
PE-3	Physical Access Control			
PE-3(1)	PHYSICAL ACCESS CONTROL / INFORMATION SYSTEM ACCESS			
PE-3(2)	PHYSICAL ACCESS CONTROL / FACILITY / INFORMATION SYSTEM BOUNDARIES			
PE-3(3)	PHYSICAL ACCESS CONTROL / CONTINUOUS GUARDS / ALARMS / MONITORING			
PE-3(4)	PHYSICAL ACCESS CONTROL / LOCKABLE CASINGS			
PE-3(5)	PHYSICAL ACCESS CONTROL / TAMPER PROTECTION			
PE-3(6)	PHYSICAL ACCESS CONTROL / FACILITY PENETRATION TESTING			
PE-4	Access Control for Transmission Medium	x	x	
PE-5	Access Control for Output Devices	x	x	
PE-5(1)	ACCESS CONTROL FOR OUTPUT DEVICES / ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS			
PE-5(2)	ACCESS CONTROL FOR OUTPUT DEVICES / ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY			
PE-5(3)	ACCESS CONTROL FOR OUTPUT DEVICES / MARKING OUTPUT DEVICES			
PE-6	Monitoring Physical Access		x	
PE-6(1)	MONITORING PHYSICAL ACCESS / INTRUSION ALARMS / SURVEILLANCE EQUIPMENT			
PE-6(2)	MONITORING PHYSICAL ACCESS / AUTOMATED INTRUSION RECOGNITION / RESPONSES			
PE-6(3)	MONITORING PHYSICAL ACCESS / VIDEO SURVEILLANCE			
PE-6(4)	MONITORING PHYSICAL ACCESS / MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS			x
PE-8	Visitor Access Records			
PE-8(1)	VISITOR ACCESS RECORDS / AUTOMATED RECORDS MAINTENANCE / REVIEW			
PE-9	Power Equipment and Cabling			
PE-9(1)	POWER EQUIPMENT AND CABLING / REDUNDANT CABLING			
PE-9(2)	POWER EQUIPMENT AND CABLING / AUTOMATIC VOLTAGE CONTROLS			

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
PE-10	Emergency Shutoff			
PE-11	Emergency Power			
PE-11(1)	EMERGENCY POWER / LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY			
PE-11(2)	EMERGENCY POWER / LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED			
PE-12	Emergency Lighting			
PE-12(1)	EMERGENCY LIGHTING / ESSENTIAL MISSIONS / BUSINESS FUNCTIONS			
PE-13	Fire Protection			
PE-13(1)	FIRE PROTECTION / DETECTION DEVICES / SYSTEMS			
PE-13(2)	FIRE PROTECTION / SUPPRESSION DEVICES / SYSTEMS			
PE-13(3)	FIRE PROTECTION / AUTOMATIC FIRE SUPPRESSION			
PE-13(4)	FIRE PROTECTION / INSPECTIONS			
PE-14	Temperature and Humidity Controls			
PE-14(1)	TEMPERATURE AND HUMIDITY CONTROLS / AUTOMATIC CONTROLS			
PE-14(2)	TEMPERATURE AND HUMIDITY CONTROLS / MONITORING WITH ALARMS / NOTIFICATIONS			
PE-15	Water Damage Protection			
PE-15(1)	WATER DAMAGE PROTECTION / AUTOMATION SUPPORT			
PE-16	Delivery and Removal			
PE-17	Alternate Work Site			
PE-18	Location of Information System Components			
PE-18(1)	LOCATION OF INFORMATION SYSTEM COMPONENTS / FACILITY SITE			
PE-19	Information Leakage			
PE-19(1)	INFORMATION LEAKAGE / NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES			
PE-20	Asset Monitoring and Tracking			

PLANNING CONTROLS

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
PL-1	Security Planning Policy and Procedures	x	x	
PL-2	System Security Plan	x	x	
PL-2(3)	SYSTEM SECURITY PLAN / PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	x	x	
PL-4	Rules of Behavior	x	x	
PL-4(1)	RULES OF BEHAVIOR / SOCIAL MEDIA AND NETWORKING RESTRICTIONS	x	x	
PL-7	Security Concept of Operations		x	
PL-8	Information Security Architecture	x	x	
PL-8(1)	INFORMATION SECURITY ARCHITECTURE / DEFENSE-IN-DEPTH			x
PL-8(2)	INFORMATION SECURITY ARCHITECTURE / SUPPLIER DIVERSITY			x
PL-9	Central Management			

PERSONNEL SECURITY CONTROLS

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
PS-1	Personnel Security Policy and Procedures			
PS-2	Position Risk Designation			
PS-3	Personnel Screening			
PS-3(1)	PERSONNEL SCREENING / CLASSIFIED INFORMATION			
PS-3(2)	PERSONNEL SCREENING / FORMAL INDOCTRINATION			
PS-3(3)	PERSONNEL SCREENING / INFORMATION WITH SPECIAL PROTECTION MEASURES			
PS-4	Personnel Termination			
PS-4(1)	PERSONNEL TERMINATION / POST-EMPLOYMENT REQUIREMENTS			
PS-4(2)	PERSONNEL TERMINATION / AUTOMATED NOTIFICATION			
PS-5	Personnel Transfer			
PS-6	Access Agreements			
PS-6(2)	ACCESS AGREEMENTS / CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION			
PS-6(3)	ACCESS AGREEMENTS / POST-EMPLOYMENT REQUIREMENTS			
PS-7	Third-Party Personnel Security			
PS-8	Personnel Sanctions			

RISK ASSESSMENT CONTROLS

CNTL NO.	CONTROL NAME Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
RA-1	Risk Assessment Policy and Procedures	x	x	
RA-2	Security Categorization			
RA-3	Risk Assessment			
RA-5	Vulnerability Scanning	x	x	
RA-5(1)	VULNERABILITY SCANNING / UPDATE TOOL CAPABILITY	x	x	
RA-5(2)	VULNERABILITY SCANNING / UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED	x	x	
RA-5(3)	VULNERABILITY SCANNING / BREADTH / DEPTH OF COVERAGE			x
RA-5(4)	VULNERABILITY SCANNING / DISCOVERABLE INFORMATION		x	
RA-5(5)	VULNERABILITY SCANNING / PRIVILEGED ACCESS	x	x	
RA-5(6)	VULNERABILITY SCANNING / AUTOMATED TREND ANALYSES			
RA-5(8)	VULNERABILITY SCANNING / REVIEW HISTORIC AUDIT LOGS			x
RA-5(10)	VULNERABILITY SCANNING / CORRELATE SCANNING INFORMATION			
RA-6	Technical Surveillance Countermeasures Survey			

SYSTEM AND SERVICES ACQUISITION CONTROLS

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SA-1	System and Services Acquisition Policy and Procedures	x	x	
SA-2	Allocation of Resources	x	x	
SA-3	System Development Life Cycle	x	x	
SA-4	Acquisition Process	x	x	
SA-4(1)	ACQUISITION PROCESS / FUNCTIONAL PROPERTIES OF SECURITY CONTROLS	x	x	
SA-4(2)	ACQUISITION PROCESS / DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS	x	x	
SA-4(3)	ACQUISITION PROCESS / DEVELOPMENT METHODS / TECHNIQUES / PRACTICES			
SA-4(5)	ACQUISITION PROCESS / SYSTEM / COMPONENT / SERVICE CONFIGURATIONS			
SA-4(6)	ACQUISITION PROCESS / USE OF INFORMATION ASSURANCE PRODUCTS			
SA-4(7)	ACQUISITION PROCESS / NIAP-APPROVED PROTECTION PROFILES			
SA-4(8)	ACQUISITION PROCESS / CONTINUOUS MONITORING PLAN			
SA-4(9)	ACQUISITION PROCESS / FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE	x	x	
SA-4(10)	ACQUISITION PROCESS / USE OF APPROVED PIV PRODUCTS	x	x	

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SA-5	Information System Documentation	x	x	
SA-8	Security Engineering Principles	x	x	
SA-9	External Information System Services	x	x	
SA-9(1)	EXTERNAL INFORMATION SYSTEMS / RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS			
SA-9(2)	EXTERNAL INFORMATION SYSTEMS / IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES	x	x	
SA-9(3)	EXTERNAL INFORMATION SYSTEMS / ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS			x
SA-9(4)	EXTERNAL INFORMATION SYSTEMS / CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS			
SA-9(5)	EXTERNAL INFORMATION SYSTEMS / PROCESSING, STORAGE, AND SERVICE LOCATION			
SA-10	Developer Configuration Management	x	x	
SA-10(1)	DEVELOPER CONFIGURATION MANAGEMENT / SOFTWARE / FIRMWARE INTEGRITY VERIFICATION			x
SA-10(2)	DEVELOPER CONFIGURATION MANAGEMENT / ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES			x
SA-10(3)	DEVELOPER CONFIGURATION MANAGEMENT / HARDWARE INTEGRITY VERIFICATION			x
SA-10(4)	DEVELOPER CONFIGURATION MANAGEMENT / TRUSTED GENERATION			
SA-10(5)	DEVELOPER CONFIGURATION MANAGEMENT / MAPPING INTEGRITY FOR VERSION CONTROL			
SA-10(6)	DEVELOPER CONFIGURATION MANAGEMENT / TRUSTED DISTRIBUTION			x
SA-11	Developer Security Testing and Evaluation	x	x	
SA-11(1)	DEVELOPER SECURITY TESTING AND EVALUATION / STATIC CODE ANALYSIS			x
SA-11(2)	DEVELOPER SECURITY TESTING AND EVALUATION / THREAT AND VULNERABILITY ANALYSES			x
SA-11(3)	DEVELOPER SECURITY TESTING AND EVALUATION / INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE			x
SA-11(4)	DEVELOPER SECURITY TESTING AND EVALUATION / MANUAL CODE REVIEWS			x
SA-11(5)	DEVELOPER SECURITY TESTING AND EVALUATION / PENETRATION TESTING			x
SA-11(6)	DEVELOPER SECURITY TESTING AND EVALUATION / ATTACK SURFACE REVIEWS			x
SA-11(7)	DEVELOPER SECURITY TESTING AND EVALUATION / VERIFY SCOPE OF TESTING / EVALUATION			x
SA-11(8)	DEVELOPER SECURITY TESTING AND EVALUATION / DYNAMIC CODE ANALYSIS			x
SA-12	Supply Chain Protection		x	
SA-12(1)	SUPPLY CHAIN PROTECTION / ACQUISITION STRATEGIES / TOOLS / METHODS			x
SA-12(2)	SUPPLY CHAIN PROTECTION / SUPPLIER REVIEWS			x

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SA-12(5)	SUPPLY CHAIN PROTECTION / LIMITATION OF HARM			
SA-12(7)	SUPPLY CHAIN PROTECTION / ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE			
SA-12(8)	SUPPLY CHAIN PROTECTION / USE OF ALL-SOURCE INTELLIGENCE			
SA-12(9)	SUPPLY CHAIN PROTECTION / OPERATIONS SECURITY			X
SA-12(10)	SUPPLY CHAIN PROTECTION / VALIDATE AS GENUINE AND NOT ALTERED			X
SA-12(11)	SUPPLY CHAIN PROTECTION / PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS			
SA-12(12)	SUPPLY CHAIN PROTECTION / INTER-ORGANIZATIONAL AGREEMENTS			
SA-12(13)	SUPPLY CHAIN PROTECTION / CRITICAL INFORMATION SYSTEM COMPONENTS			
SA-12(14)	SUPPLY CHAIN PROTECTION / IDENTITY AND TRACEABILITY			X
SA-12(15)	SUPPLY CHAIN PROTECTION / PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES			
SA-13	Trustworthiness			X
SA-14	Criticality Analysis			
SA-15	Development Process, Standards, and Tools		X	
SA-15(1)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / QUALITY METRICS			X
SA-15(2)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / SECURITY TRACKING TOOLS			X
SA-15(3)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / CRITICALITY ANALYSIS			X
SA-15(4)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / THREAT MODELING / VULNERABILITY ANALYSIS			X
SA-15(5)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / ATTACK SURFACE REDUCTION			X
SA-15(6)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / CONTINUOUS IMPROVEMENT			X
SA-15(7)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / AUTOMATED VULNERABILITY ANALYSIS			X
SA-15(8)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / REUSE OF THREAT / VULNERABILITY INFORMATION			
SA-15(9)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / USE OF LIVE DATA			
SA-15(10)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / INCIDENT RESPONSE PLAN			
SA-15(11)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS / ARCHIVE INFORMATION SYSTEM / COMPONENT			
SA-16	Developer-Provided Training		X	
SA-17	Developer Security Architecture and Design		X	

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SA-17(1)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN / FORMAL POLICY MODEL			X
SA-17(2)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN / SECURITY-RELEVANT COMPONENTS			X
SA-17(3)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN / FORMAL CORRESPONDENCE			
SA-17(4)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN / INFORMAL CORRESPONDENCE			
SA-17(5)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN / CONCEPTUALLY SIMPLE DESIGN			
SA-17(6)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN / STRUCTURE FOR TESTING			
SA-17(7)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN / STRUCTURE FOR LEAST PRIVILEGE			
SA-18	Tamper Resistance and Detection			X
SA-18(1)	TAMPER RESISTANCE AND DETECTION / MULTIPLE PHASES OF SDLC			X
SA-18(2)	TAMPER RESISTANCE AND DETECTION / INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES			X
SA-19	Component Authenticity			X
SA-19(1)	COMPONENT AUTHENTICITY / ANTI-COUNTERFEIT TRAINING			X
SA-19(2)	COMPONENT AUTHENTICITY / CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR			
SA-19(3)	COMPONENT AUTHENTICITY / COMPONENT DISPOSAL			
SA-19(4)	COMPONENT AUTHENTICITY / ANTI-COUNTERFEIT SCANNING			X
SA-20	Customized Development of Critical Components			
SA-21	Developer Screening			X
SA-21(1)	DEVELOPER SCREENING / VALIDATION OF SCREENING			X
SA-22	Unsupported System Components			X
SA-22(1)	UNSUPPORTED SYSTEM COMPONENTS / ALTERNATIVE SOURCES FOR CONTINUED SUPPORT			X

SYSTEM AND COMMUNICATIONS PROTECTION CONTROLS

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SC-1	System and Communications Protection Policy and Procedures	X	X	
SC-2	Application Partitioning	X	X	
SC-2(1)	APPLICATION PARTITIONING / INTERFACES FOR NON-PRIVILEGED USERS			X
SC-3	Security Function Isolation		X	
SC-3(1)	SECURITY FUNCTION ISOLATION / HARDWARE SEPARATION			X

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SC-3(2)	SECURITY FUNCTION ISOLATION / ACCESS / FLOW CONTROL FUNCTIONS			X
SC-3(3)	SECURITY FUNCTION ISOLATION / MINIMIZE NONSECURITY FUNCTIONALITY			
SC-3(4)	SECURITY FUNCTION ISOLATION / MODULE COUPLING AND COHESIVENESS			
SC-3(5)	SECURITY FUNCTION ISOLATION / LAYERED STRUCTURES			
SC-4	Information in Shared Resources	X	X	
SC-4(2)	INFORMATION IN SHARED RESOURCES / PERIODS PROCESSING			
SC-5	Denial of Service Protection	X	X	
SC-5(1)	DENIAL OF SERVICE PROTECTION / RESTRICT INTERNAL USERS			
SC-5(2)	DENIAL OF SERVICE PROTECTION / EXCESS CAPACITY / BANDWIDTH / REDUNDANCY			
SC-5(3)	DENIAL OF SERVICE PROTECTION / DETECTION / MONITORING			
SC-6	Resource Availability			
SC-7	Boundary Protection	X	X	
SC-7(3)	BOUNDARY PROTECTION / ACCESS POINTS	X	X	
SC-7(4)	BOUNDARY PROTECTION / EXTERNAL TELECOMMUNICATIONS SERVICES	X	X	
SC-7(5)	BOUNDARY PROTECTION / DENY BY DEFAULT / ALLOW BY EXCEPTION	X	X	
SC-7(7)	BOUNDARY PROTECTION / PREVENT SPLIT TUNNELING FOR REMOTE DEVICES	X	X	
SC-7(8)	BOUNDARY PROTECTION / ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS		X	
SC-7(9)	BOUNDARY PROTECTION / RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC			
SC-7(10)	BOUNDARY PROTECTION / PREVENT UNAUTHORIZED EXFILTRATION			X
SC-7(11)	BOUNDARY PROTECTION / RESTRICT INCOMING COMMUNICATIONS TRAFFIC			X
SC-7(12)	BOUNDARY PROTECTION / HOST-BASED PROTECTION			X
SC-7(13)	BOUNDARY PROTECTION / ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS			
SC-7(14)	BOUNDARY PROTECTION / PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS		X	
SC-7(15)	BOUNDARY PROTECTION / ROUTE PRIVILEGED NETWORK ACCESSES			
SC-7(16)	BOUNDARY PROTECTION / PREVENT DISCOVERY OF COMPONENTS / DEVICES			
SC-7(17)	BOUNDARY PROTECTION / AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS			

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SC-7(18)	BOUNDARY PROTECTION / FAIL SECURE		X	
SC-7(19)	BOUNDARY PROTECTION / BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS			
SC-7(20)	BOUNDARY PROTECTION / DYNAMIC ISOLATION / SEGREGATION			X
SC-7(21)	BOUNDARY PROTECTION / ISOLATION OF INFORMATION SYSTEM COMPONENTS		X	
SC-7(22)	BOUNDARY PROTECTION / SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS			
SC-7(23)	BOUNDARY PROTECTION / DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE			
SC-8	Transmission Confidentiality and Integrity	X	X	
SC-8(1)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY / CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION	X	X	
SC-8(2)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY / PRE / POST TRANSMISSION HANDLING			
SC-8(3)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY / CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS			
SC-8(4)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY / CONCEAL / RANDOMIZE COMMUNICATIONS			
SC-10	Network Disconnect	X	X	
SC-11	Trusted Path			X
SC-11(1)	TRUSTED PATH / LOGICAL ISOLATION			X
SC-12	Cryptographic Key Establishment and Management	X	X	
SC-12(1)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT / AVAILABILITY		X	
SC-12(2)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT / SYMMETRIC KEYS			
SC-12(3)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT / ASYMMETRIC KEYS			
SC-13	Cryptographic Protection	X	X	
SC-15	Collaborative Computing Devices	X	X	
SC-15(1)	COLLABORATIVE COMPUTING DEVICES / PHYSICAL DISCONNECT			
SC-15(3)	COLLABORATIVE COMPUTING DEVICES / DISABLING / REMOVAL IN SECURE WORK AREAS			
SC-15(4)	COLLABORATIVE COMPUTING DEVICES / EXPLICITLY INDICATE CURRENT PARTICIPANTS			
SC-16	Transmission of Security Attributes			X
SC-16(1)	TRANSMISSION OF SECURITY ATTRIBUTES / INTEGRITY VALIDATION			X
SC-17	Public Key Infrastructure Certificates	X	X	
SC-18	Mobile Code	X	X	
SC-18(1)	MOBILE CODE / IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS			X

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SC-18(2)	MOBILE CODE / ACQUISITION / DEVELOPMENT / USE			
SC-18(3)	MOBILE CODE / PREVENT DOWNLOADING / EXECUTION			X
SC-18(4)	MOBILE CODE / PREVENT AUTOMATIC EXECUTION			X
SC-18(5)	MOBILE CODE / ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS			
SC-19	Voice Over Internet Protocol	X	X	
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	X	X	
SC-20(2)	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) / DATA ORIGIN / INTEGRITY			X
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	X	X	
SC-22	Architecture and Provisioning for Name/Address Resolution Service	X	X	
SC-23	Session Authenticity	X	X	
SC-23(1)	SESSION AUTHENTICITY / INVALIDATE SESSION IDENTIFIERS AT LOGOUT			
SC-23(3)	SESSION AUTHENTICITY / UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION			
SC-23(5)	SESSION AUTHENTICITY / ALLOWED CERTIFICATE AUTHORITIES			
SC-24	Fail in Known State		X	
SC-25	Thin Nodes			
SC-26	Honeypots			X
SC-27	Platform-Independent Applications			
SC-28	Protection of Information at Rest	X	X	
SC-28(1)	PROTECTION OF INFORMATION AT REST / CRYPTOGRAPHIC PROTECTION			X
SC-28(2)	PROTECTION OF INFORMATION AT REST / OFF-LINE STORAGE			
SC-29	Heterogeneity			
SC-29(1)	HETEROGENEITY / VIRTUALIZATION TECHNIQUES			
SC-30	Concealment and Misdirection			
SC-30(2)	CONCEALMENT AND MISDIRECTION / RANDOMNESS			
SC-30(3)	CONCEALMENT AND MISDIRECTION / CHANGE PROCESSING / STORAGE LOCATIONS			
SC-30(4)	CONCEALMENT AND MISDIRECTION / MISLEADING INFORMATION			
SC-30(5)	CONCEALMENT AND MISDIRECTION / CONCEALMENT OF SYSTEM COMPONENTS			
SC-31	Covert Channel Analysis			

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SC-31(1)	COVERT CHANNEL ANALYSIS / TEST COVERT CHANNELS FOR EXPLOITABILITY			
SC-31(2)	COVERT CHANNEL ANALYSIS / MAXIMUM BANDWIDTH			
SC-31(3)	COVERT CHANNEL ANALYSIS / MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS			
SC-32	Information System Partitioning			
SC-34	Non-Modifiable Executable Programs			
SC-34(1)	NON-MODIFIABLE EXECUTABLE PROGRAMS / NO WRITABLE STORAGE			
SC-34(2)	NON-MODIFIABLE EXECUTABLE PROGRAMS / INTEGRITY PROTECTION / READ-ONLY MEDIA			
SC-34(3)	NON-MODIFIABLE EXECUTABLE PROGRAMS / HARDWARE-BASED PROTECTION			
SC-35	Honeyclients			
SC-36	Distributed Processing and Storage			
SC-36(1)	DISTRIBUTED PROCESSING AND STORAGE / POLLING TECHNIQUES			
SC-37	Out-of-Band Channels			
SC-37(1)	OUT-OF-BAND CHANNELS / ENSURE DELIVERY / TRANSMISSION			
SC-38	Operations Security			x
SC-39	Process Isolation	x	x	
SC-39(1)	PROCESS ISOLATION / HARDWARE SEPARATION			
SC-39(2)	PROCESS ISOLATION / THREAD ISOLATION			
SC-40	Wireless Link Protection			
SC-40(1)	WIRELESS LINK PROTECTION / ELECTROMAGNETIC INTERFERENCE			
SC-40(2)	WIRELESS LINK PROTECTION / REDUCE DETECTION POTENTIAL			
SC-40(3)	WIRELESS LINK PROTECTION / IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION			
SC-40(4)	WIRELESS LINK PROTECTION / SIGNAL PARAMETER IDENTIFICATION			
SC-41	Port and I/O Device Access			x
SC-42	Sensor Capability and Data			
SC-42(1)	SENSOR CAPABILITY AND DATA / REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES			
SC-42(2)	SENSOR CAPABILITY AND DATA / AUTHORIZED USE			
SC-42(3)	SENSOR CAPABILITY AND DATA / PROHIBIT USE OF DEVICES			
SC-43	Usage Restrictions			
SC-44	Detonation Chambers			

SYSTEM AND INFORMATION INTEGRITY CONTROLS

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SI-1	System and Information Integrity Policy and Procedures	x	x	
SI-2	Flaw Remediation	x	x	
SI-2(1)	FLAW REMEDIATION / CENTRAL MANAGEMENT		x	
SI-2(2)	FLAW REMEDIATION / AUTOMATED FLAW REMEDIATION STATUS	x	x	
SI-2(3)	FLAW REMEDIATION / TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS			x
SI-2(5)	FLAW REMEDIATION / AUTOMATIC SOFTWARE / FIRMWARE UPDATES			
SI-2(6)	FLAW REMEDIATION / REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE			
SI-3	Malicious Code Protection	x	x	
SI-3(1)	MALICIOUS CODE PROTECTION / CENTRAL MANAGEMENT	x	x	
SI-3(2)	MALICIOUS CODE PROTECTION / AUTOMATIC UPDATES	x	x	
SI-3(4)	MALICIOUS CODE PROTECTION / UPDATES ONLY BY PRIVILEGED USERS			
SI-3(6)	MALICIOUS CODE PROTECTION / TESTING / VERIFICATION			
SI-3(7)	MALICIOUS CODE PROTECTION / NONSIGNATURE-BASED DETECTION			x
SI-3(8)	MALICIOUS CODE PROTECTION / DETECT UNAUTHORIZED COMMANDS		x	
SI-3(9)	MALICIOUS CODE PROTECTION / AUTHENTICATE REMOTE COMMANDS			
SI-3(10)	MALICIOUS CODE PROTECTION / MALICIOUS CODE ANALYSIS		x	
SI-4	Information System Monitoring	x	x	
SI-4(1)	INFORMATION SYSTEM MONITORING / SYSTEM-WIDE INTRUSION DETECTION SYSTEM			x
SI-4(2)	INFORMATION SYSTEM MONITORING / AUTOMATED TOOLS FOR REAL-TIME ANALYSIS	x	x	
SI-4(3)	INFORMATION SYSTEM MONITORING / AUTOMATED TOOL INTEGRATION			
SI-4(4)	INFORMATION SYSTEM MONITORING / INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	x	x	
SI-4(5)	INFORMATION SYSTEM MONITORING / SYSTEM-GENERATED ALERTS	x	x	
SI-4(7)	INFORMATION SYSTEM MONITORING / AUTOMATED RESPONSE TO SUSPICIOUS EVENTS			
SI-4(9)	INFORMATION SYSTEM MONITORING / TESTING OF MONITORING TOOLS			x

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SI-4(10)	INFORMATION SYSTEM MONITORING / VISIBILITY OF ENCRYPTED COMMUNICATIONS		X	
SI-4(11)	INFORMATION SYSTEM MONITORING / ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES		X	
SI-4(12)	INFORMATION SYSTEM MONITORING / AUTOMATED ALERTS			X
SI-4(13)	INFORMATION SYSTEM MONITORING / ANALYZE TRAFFIC / EVENT PATTERNS			X
SI-4(14)	INFORMATION SYSTEM MONITORING / WIRELESS INTRUSION DETECTION			X
SI-4(15)	INFORMATION SYSTEM MONITORING / WIRELESS TO WIRELINE COMMUNICATIONS			
SI-4(16)	INFORMATION SYSTEM MONITORING / CORRELATE MONITORING INFORMATION			
SI-4(17)	INFORMATION SYSTEM MONITORING / INTEGRATED SITUATIONAL AWARENESS			X
SI-4(18)	INFORMATION SYSTEM MONITORING / ANALYZE TRAFFIC / COVERT EXFILTRATION			
SI-4(19)	INFORMATION SYSTEM MONITORING / INDIVIDUALS POSING GREATER RISK			X
SI-4(20)	INFORMATION SYSTEM MONITORING / PRIVILEGED USER		X	
SI-4(21)	INFORMATION SYSTEM MONITORING / PROBATIONARY PERIODS			
SI-4(22)	INFORMATION SYSTEM MONITORING / UNAUTHORIZED NETWORK SERVICES			X
SI-4(23)	INFORMATION SYSTEM MONITORING / HOST-BASED DEVICES			X
SI-4(24)	INFORMATION SYSTEM MONITORING / INDICATORS OF COMPROMISE			X
SI-5	Security Alerts, Advisories, and Directives	X	X	
SI-5(1)	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES / AUTOMATED ALERTS AND ADVISORIES		X	
SI-6	Security Function Verification		X	
SI-6(2)	SECURITY FUNCTION VERIFICATION / AUTOMATION SUPPORT FOR DISTRIBUTED TESTING			
SI-6(3)	SECURITY FUNCTION VERIFICATION / REPORT VERIFICATION RESULTS		X	
SI-7	Software, Firmware, and Information Integrity	X	X	
SI-7(1)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / INTEGRITY CHECKS	X	X	
SI-7(2)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS		X	
SI-7(3)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / CENTRALLY MANAGED INTEGRITY TOOLS			
SI-7(5)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS		X	

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SI-7(6)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / CRYPTOGRAPHIC PROTECTION			
SI-7(7)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / INTEGRATION OF DETECTION AND RESPONSE	x	x	
SI-7(8)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / AUDITING CAPABILITY FOR SIGNIFICANT EVENTS			
SI-7(9)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / VERIFY BOOT PROCESS			
SI-7(10)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / PROTECTION OF BOOT FIRMWARE			
SI-7(11)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES			
SI-7(12)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / INTEGRITY VERIFICATION			x
SI-7(13)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / CODE EXECUTION IN PROTECTED ENVIRONMENTS			
SI-7(14)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / BINARY OR MACHINE EXECUTABLE CODE		x	
SI-7(15)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / CODE AUTHENTICATION			
SI-7(16)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY / TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION			
SI-8	Spam Protection	x	x	
SI-8(1)	SPAM PROTECTION / CENTRAL MANAGEMENT	x	x	
SI-8(2)	SPAM PROTECTION / AUTOMATIC UPDATES	x	x	
SI-8(3)	SPAM PROTECTION / CONTINUOUS LEARNING CAPABILITY			
SI-10	Information Input Validation	x	x	
SI-10(1)	INFORMATION INPUT VALIDATION / MANUAL OVERRIDE CAPABILITY			
SI-10(2)	INFORMATION INPUT VALIDATION / REVIEW / RESOLUTION OF ERRORS			
SI-10(3)	INFORMATION INPUT VALIDATION / PREDICTABLE BEHAVIOR			x
SI-10(4)	INFORMATION INPUT VALIDATION / REVIEW / TIMING INTERACTIONS			
SI-10(5)	INFORMATION INPUT VALIDATION / REVIEW / RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS			x
SI-11	Error Handling	x	x	
SI-12	Information Handling and Retention	x	x	
SI-13	Predictable Failure Prevention			
SI-13(1)	PREDICTABLE FAILURE PREVENTION / TRANSFERRING COMPONENT RESPONSIBILITIES			
SI-13(3)	PREDICTABLE FAILURE PREVENTION / MANUAL TRANSFER BETWEEN COMPONENTS			

CNTL NO.	Control Name Control Enhancement Name	CONTROL SETS		
		Set II	Set I	DBT
SI-13(4)	PREDICTABLE FAILURE PREVENTION / STANDBY COMPONENT INSTALLATION / NOTIFICATION			
SI-13(5)	PREDICTABLE FAILURE PREVENTION / FAILOVER CAPABILITY			
SI-14	Non-Persistence			
SI-14(1)	NON-PERSISTENCE / REFRESH FROM TRUSTED SOURCES			
SI-15	Information Output Filtering			
SI-16	Memory Protection	x	x	
SI-17	Fail-Safe Procedures			