DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, DC

29 February 2024

MEMORANDUM FOR AIR FORCE CIVIL ENGINEER CENTER

FROM: HQ USAF/A4C
1260 Air Force Pentagon
Washington, DC 20330-1260

SUBJECT: Civil Engineer Control Systems (CECS) Baseline Security Controls

References: (a) Civil Engineer (CE) Facility Related Control Systems (FRCS) Baseline Security Controls 10 September 2018.
(b) DAFGM2023-32-01, Civil Engineer Control Systems Cybersecurity
(c) NIST SP 800-53B - Control Baselines for Information Systems and Organizations.
(d) NIST SP 800-82 r2 - Guide to Industrial Control Systems (ICS) Security.
(e) Standalone Information Systems (SIS)/Closed Restricted Network (CRN) Assessment and Authorization (A&A) Tactics, Techniques, and Procedural Assessment Guide Version 2.0
(f) DAF Organizational Risk Tolerance Baseline (ORTB), from the DAF Risk Management Framework Knowledge Service

Risk Management Framework principles require the use of NIST 800-53 Security Controls that are tailored to the information system type on which they are applied. After considerable experience in applying the 47 baseline controls in place since 2018, the CECS Enterprise is now sufficiently mature to apply additional cybersecurity controls to further harden our systems against increasing threats. Effective with the start of the new CECS Cybersecurity contract in 29 February, 2024, for all new accreditations, renewal accreditations, and annual security reviews, the following sets of baseline controls apply, with the expectation that further tailoring will be applied based on specific system/mission requirements.

Individual controls are listed on the attached table.

a. CECS with no IT components: 34 controls.
b. CECS, Stand-Alone with Low categorization: 82 controls.
c. CECS, Stand-Alone with Moderate categorization: 90 controls.
d. CECS, Stand-Alone with High categorization: 97 controls.
e. CECS, COIN v2 Connected with Low categorization: 189 controls.
f. CECS, COIN v2 Connected with Moderate categorization: 195 controls.

These controls were carefully evaluated to provide increased hardening guidance to the bases, take advantage of inherited controls, and eliminate administrative controls that contribute poorly towards system hardening. As a consequence of working smarter, my expectation is that after a transition period, the revised control set will not involve more work at the bases for accreditations than is currently already being done.

Questions or concerns are to be directed to Mr. Mark McClellan, GS-14, AFCEC/COOI at DSN: 523-6290, commercial: (405)210-6166 or mark.mcclellan@us.af.mil .

DENTINO.DAVID.H.1126570488 Digitally signed by DENTINO.DAVID.H.1126570488 Date: 2024.02.29 14:06:38 -05'00'

DAVID H. DENTINO, SES, DAF
Authorizing Official, CE Control Systems

Attachments:
1. Table 1, CECS Baseline Controls Breakdown, Part 1
2. Table 2, CECS Baseline Controls Breakdown, Part 2
3. Table 3, CECS Baseline Controls Breakdown, Part 3

Table 1 CECS Baseline Controls Breakdown, Part 1

			System Configuration						
				Interconnection Type					
	Controls Validated via Checklist		No IT Control System	Stand Alone Control System			COINv2 Interconnected Control System		
202	16	40	34	82	90	97	189	195	
Total Controls	ConMon Controls	ASR Core Controls	Low	Low	Moderate	High	Low	Moderate	Control Category/Family
AC-1		AC-1	AC-1	AC-1	AC-1	AC-1	AC-1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES
AC-2	AC-2	AC-2		AC-2	AC-2	AC-2	AC-2	AC-2	ACCOUNT MANAGEMENT
AC-2(3)							AC-2(3)	AC-2(3)	ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS
AC-2(5)							AC-2(5)	AC-2(5)	ACCOUNT MANAGEMENT | INACTIVITY LOGOUT
AC-2(7)				AC-2(7)	AC-2(7)	AC-2(7)	AC-2(7)	AC-2(7)	ROLE-BASED SCHEMES
AC-2(9)							AC-2(9)	AC-2(9)	ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS
AC-2(12)							AC-2(12)	AC-2(12)	ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE
AC-2(13)							AC-2(13)	AC-2(13)	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS
AC-4	AC-4	AC-4			AC-4	AC-4		AC-4	INFORMATION FLOW ENFORCEMENT
AC-5				AC-5	AC-5	AC-5	AC-5	AC-5	SEPARATION OF DUTIES
AC-6	AC-6	AC-6			AC-6	AC-6	AC-6	AC-6	LEAST PRIVILEGE
AC-6(1)							AC-6(1)	AC-6(1)	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS
AC-6(2)							AC-6(2)	AC-6(2)	LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS
AC-6(5)				AC-6(5)	AC-6(5)	AC-6(5)	AC-6(5)	AC-6(5)	LEAST PRIVILEGE | PRIVILEGED ACCOUNTS
AC-6(7)							AC-6(7)	AC-6(7)	LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES
AC-7				AC-7	AC-7	AC-7	AC-7	AC-7	UNSUCCESSFUL LOGON ATTEMPTS
AC-11				AC-11	AC-11	AC-11	AC-11	AC-11	SESSION LOCK
AC-14							AC-14	AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
AC-17							AC-17	AC-17	REMOTE ACCESS
AC-17(1)							AC-17(1)	AC-17(1)	REMOTE ACCESS | AUTOMATED MONITORING / CONTROL
AC-17(3)							AC-17(3)	AC-17(3)	REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS
AC-17(4)							AC-17(4)	AC-17(4)	REMOTE ACCESS | PRIVILEGED COMMANDS/ ACCESS
AC-17(6)							AC-17(6)	AC-17(6)	REMOTE ACCESS | PROTECTION OF INFORMATION
AC-18		AC-18		AC-18	AC-18	AC-18	AC-18	AC-18	WIRELESS ACCESS
AC-18(1)				AC-18(1)	AC-18(1)	AC-18(1)	AC-18(1)	AC-18(1)	WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION
AC-18(3)				AC-18(3)	AC-18(3)	AC-18(3)	AC-18(3)	AC-18(3)	WIRELESS ACCESS | DISABLE WIRELESS NETWORKING
AC-19							AC-19	AC-19	ACCESS CONTROL FOR MOBILE DEVICES
AC-20							AC-20	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS
AC-20(2)							AC-20(2)	AC-20(2)	USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES
AC-20(3)							AC-20(3)	AC-20(3)	USE OF EXTERNAL INFORMATION SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES
AC-23							AC-23	AC-23	DATA MINING PROTECTION
AU-2				AU-2	AU-2	AU-2	AU-2	AU-2	AUDIT EVENTS
AU-2(3)				AU-2(3)	AU-2(3)	AU-2(3)	AU-2(3)	AU-2(3)	AUDIT EVENTS | REVIEWS AND UPDATES
AU-4							AU-4	AU-4	AUDIT STORAGE CAPACITY
AU-6							AU-6	AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-6(1)							AU-6(1)	AU-6(1)	AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION
AU-6(3)							AU-6(3)	AU-6(3)	AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES
AU-6(4)							AU-6(4)	AU-6(4)	AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS
AU-6(10)							AU-6(10)	AU-6(10)	AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT
AU-7							AU-7	AU-7	AUDIT REDUCTION AND REPORT GENERATION
AU-7(1)							AU-7(1)	AU-7(1)	AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING
AU-8							AU-8	AU-8	TIME STAMPS
AU-9							AU-9	AU-9	PROTECTION OF AUDIT INFORMATION
AU-9(4)							AU-9(4)	AU-9(4)	PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS
AU-11							AU-11	AU-11	AUDIT RECORD RETENTION
AU-11(1)							AU-11(1)	AU-11(1)	AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY
AU-12(1)							AU-12(1)	AU-12(1)	AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL
AU-14							AU-14	AU-14	SESSION AUDIT
AU-14(3)							AU-14(3)	AU-14(3)	SESSION AUDIT | REMOTE VIEWING / LISTENING
AT-1		AT-1	AT-1	AT-1	AT-1	AT-1	AT-1	AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
AT-2			AT-2	AT-2	AT-2	AT-2	AT-2	AT-2	SECURITY AWARENESS TRAINING
AT-3							AT-3	AT-3	ROLE-BASED SECURITY TRAINING
AT-3(2)							AT-3(2)	AT-3(2)	SECURITY TRAINING | PHYSICAL SECURITY CONTROLS
AT-3(4)							AT-3(4)	AT-3(4)	SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR
AT-4		AT-4	AT-4	AT-4	AT-4	AT-4	AT-4	AT-4	SECURITY TRAINING RECORDS
CM-1		CM-1	CM-1	CM-1	CM-1	CM-1	CM-1	CM-1	CONFIGURATION MANAGEMENT POLICY & PROCEDURES
CM-2		CM-2	CM-2	CM-2	CM-2	CM-2	CM-2	CM-2	BASELINE CONFIGURATION
CM-3	CM-3	CM-3		CM-3	CM-3	CM-3	CM-3	CM-3	CONFIGURATION CHANGE CONTROL
CM-5		CM-5		CM-5	CM-5	CM-5	CM-5	CM-5	ACCESS RESTRICTIONS FOR CHANGE
CM-5(5)							CM-5(5)	CM-5(5)	ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES
CM-6	CM-6	CM-6		CM-6	CM-6	CM-6	CM-6	CM-6	CONFIGURATION SETTINGS
CM-7		CM-7		CM-7	CM-7	CM-7	CM-7	CM-7	LEAST FUNCTIONALITY
CM-7(3)							CM-7(3)	CM-7(3)	LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE
CM-7(5)				CM-7(5)	CM-7(5)	CM-7(5)	CM-7(5)	CM-7(5)	LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING
CM-8	CM-8	CM-8	CM-8	CM-8	CM-8	CM-8	CM-8	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY
CM-9				CM-9	CM-9	CM-9	CM-9	CM-9	CONFIGURATION MANAGEMENT PLAN
CM-10		CM-10		CM-10	CM-10	CM-10	CM-10	CM-10	SOFTWARE USAGE RESTRICTIONS
CM-10(1)							CM-10(1)	CM-10(1)	SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE
CM-11	CM-11			CM-11	CM-11	CM-11	CM-11	CM-11	USER-INSTALLED SOFTWARE
CM-11(2)				CM-11(2)	CM-11(2)	CM-11(2)	CM-11(2)	CM-11(2)	USER-INSTALLED SOFTWARE | PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS
CP-1		CP-1	CP-1	CP-1	CP-1	CP-1	CP-1	CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES
CP-2			CP-2	CP-2	CP-2	CP-2	CP-2	CP-2	CONTINGENCY PLAN
CP-2(1)		CP-2(1)	CP-2(1)	CP-2(1)	CP-2(1)	CP-2(1)	CP-2(1)	CP-2(1)	CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS
CP-2(8)					CP-2(8)	CP-2(8)	CP-2(8)	CP-2(8)	IDENTIFY CRITICAL ASSETS

Table 2 CECS Baseline Controls Breakdown, Part 2

			System Configuration						
				Interconnection Type					
	Controls Validated via Checklist		No IT Control System	Stand Alone Control System			COINv2 Interconnected Control System		
202	16	40	34	82	90	97	189	195	
Total Controls	ConMon Controls	ASR Core Controls	Low	Low	Moderate	High	Low	Moderate	Control Category/Family
CP-6					CP-6	CP-6		CP-6	ALTERNATE STORAGE SITE
CP-8							CP-8	CP-8	TELECOMMUNICATIONS SERVICES
CP-8(1)							CP-8(1)	CP-8(1)	TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS
CP-8(2)							CP-8(2)	CP-8(2)	TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE
CP-9	CP-9				CP-9	CP-9		CP-9	SYSTEM BACKUP
CP-10					CP-10	CP-10		CP-10	SYSTEM RECOVERY AND RECONSTITUTION
IA-1		IA-1	IA-1	IA-1	IA-1	IA-1	IA-1	IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
IA-2				IA-2	IA-2	IA-2	IA-2	IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(11)							IA-2(11)	IA-2(11)	IDENTIFICATION AND AUTHENTICATIOIN | REMOTE ACCESS - SEPARATE DEVICE
IA-3	IA-3			IA-3	IA-3	IA-3	IA-3	IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION
IA-4		IA-4		IA-4	IA-4	IA-4	IA-4	IA-4	IDENTIFIER MANAGEMENT
IA-4(4)							IA-4(4)	IA-4(4)	IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS
IA-5		IA-5		IA-5	IA-5	IA-5	IA-5	IA-5	AUTHENTICATOR MANAGEMENT
IA-5(1)				IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)	IA-5(1)	PASSWORD-BASED AUTHENTICATION
IA-5(3)							IA-5(3)	IA-5(3)	AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION
IA-5(4)							IA-5(4)	IA-5(4)	AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION
IA-5(7)							IA-5(7)	IA-5(7)	AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS
IA-5(8)				IA-5(8)	IA-5(8)	IA-5(8)	IA-5(8)	IA-5(8)	MULTIPLE INFORMATION SYSTEM ACCOUNTS
IA-5(11)				IA-5(11)	IA-5(11)	IA-5(11)	IA-5(11)	IA-5(11)	HARDWARE TOKEN-BASED AUTHENTICATION
IA-5(14)							IA-5(14)	IA-5(14)	MANAGING CONTENT OF PKI TRUST STORES
IR-1		IR-1	IR-1	IR-1	IR-1	IR-1	IR-1	IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES
IR-2		IR-2	IR-2	IR-2	IR-2	IR-2	IR-2	IR-2	INCIDENT RESPONSE TRAINING
IR-3		IR-3		IR-3	IR-3	IR-3	IR-3	IR-3	INCIDENT RESPONSE TESTING
IR-4		IR-4		IR-4	IR-4	IR-4	IR-4	IR-4	INCIDENT HANDLING
IR-4(8)				IR-4(8)	IR-4(8)	IR-4(8)	IR-4(8)	IR-4(8)	CORRELATION WITH EXTERNAL ORGANIZATIONS
IR-5			IR-5	IR-5	IR-5	IR-5	IR-5	IR-5	INCIDENT MONITORING
IR-6				IR-6	IR-6	IR-6	IR-6	IR-6	INCIDENT REPORTING
IR-7				IR-7	IR-7	IR-7	IR-7	IR-7	INCIDENT RESPONSE ASSISTANCE
IR-8		IR-8	IR-8	IR-8	IR-8	IR-8	IR-8	IR-8	INCIDENT RESPONSE PLAN
IR-9(2)		IR-9		IR-9	IR-9	IR-9	IR-9	IR-9	INFORMATION SPILLAGE RESPONSE
IR-9(2)							IR-9(2)	IR-9(2)	INFORMATION SPILLAGE RESPONSE | TRAINING
IR-10							IR-10	IR-10	INTEGRATED INFORMATION SECURITY ANALYSIS TEAM
MA-1				MA-1	MA-1	MA-1	MA-1	MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES
MA-2				MA-2	MA-2	MA-2	MA-2	MA-2	CONTROLLED MAINTENANCE
MA-3				MA-3	MA-3	MA-3	MA-3	MA-3	MAINTENANCE TOOLS
MA-4							MA-4	MA-4	NONLOCAL MAINTENANCE
MA-5							MA-5	MA-5	MAINTENANCE PERSONNEL
MP-1		MP-1	MP-1	MP-1	MP-1	MP-1	MP-1	MP-1	MEDIA PROTECTION POLICY AND PROCEDURES
MP-6				MP-6	MP-6	MP-6	MP-6	MP-6	MEDIA SANITIZATION
MP-7				MP-7	MP-7	MP-7	MP-7	MP-7	MEDIA USE
MP-7(1)							MP-7(1)	MP-7(1)	MEDIA USE | PROHIBIT USE WITHOUT OWNER
PE-1		PE-1	PE-1	PE-1	PE-1	PE-1	PE-1	PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
PE-2	PE-2			PE-2	PE-2	PE-2	PE-2	PE-2	PHYSICAL ACCESS AUTHORIZATIONS
PE-3	PE-3			PE-3	PE-3	PE-3	PE-3	PE-3	PHYSICAL ACCESS CONTROL
PE-6			PE-6	PE-6	PE-6	PE-6	PE-6	PE-6	MONITORING PHYSICAL ACCESS
PE-8	PE-8		PE-8	PE-8	PE-8	PE-8	PE-8	PE-8	VISITOR ACCESS RECORDS
PE-9						PE-9			POWER EQUIPMENT AND CABLING
PE-10						PE-10			EMERGENCY SHUTOFF
PE-11					PE-11	PE-11		PE-11	EMERGENCY POWER
PE-11(2)						PE-11(2)			Long-Term Alternate Power Supply - Self Contained
PE-16			PE-16	PE-16	PE-16	PE-16	PE-16	PE-16	DELIVERY AND REMOVAL
PL-1		PL-1	PL-1	PL-1	PL-1	PL-1	PL-1	PL-1	SECURITY PLANNING POLICY AND PROCEDURES
PL-2		PL-2	PL-2	PL-2	PL-2	PL-2	PL-2	PL-2	SYSTEM SECURITY PLAN
PL-4				PL-4	PL-4	PL-4	PL-4	PL-4	RULES OF BEHAVIOR
PL-4(1)							PL-4(1)	PL-4(1)	RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS
PL-7						PL-7			Security Concept of Operations
PM-1		PM-1	PM-1	PM-1	PM-1	PM-1	PM-1	PM-1	INFORMATION SECURITY PROGRAM PLAN
PM-2			PM-2	PM-2	PM-2	PM-2	PM-2	PM-2	SENIOR INFORMATION SECURITY OFFICER
PM-4			PM-4	PM-4	PM-4	PM-4	PM-4	PM-4	PLANS OF ACTION AND MILESTONES PROCESS
PM-13			PM-13	PM-13	PM-13	PM-13	PM-13	PM-13	INFORMATION SECURITY WORKFORCE
PS-3							PS-3	PS-3	PERSONNEL SCREENING
PS-4							PS-4	PS-4	PERSONNEL TERMINATION
PS-5							PS-5	PS-5	PERSONNEL TRANSFER
PS-6							PS-6	PS-6	ACCESS AGREEMENTS
PS-7							PS-7	PS-7	THIRD-PARTY PERSONNEL SECURITY
PS-8							PS-8	PS-8	PERSONNEL SANCTIONS
RA-1		RA-1	RA-1	RA-1	RA-1	RA-1	RA-1	RA-1	RISK ASSESSMENT POLICY AND PROCEDURES
RA-2			RA-2	RA-2	RA-2	RA-2	RA-2	RA-2	SECURITY CATEGORIZATION
RA-3			RA-3	RA-3	RA-3	RA-3	RA-3	RA-3	RISK ASSESSMENT
RA-5	RA-5			RA-5	RA-5	RA-5	RA-5	RA-5	VULNERABILITY MONITORING AND SCANNING
RA-5(1)							RA-5(1)	RA-5(1)	VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY
RA-5(2)				RA-5(2)	RA-5(2)	RA-5(2)	RA-5(2)	RA-5(2)	UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED
RA-5(5)				RA-5(5)	RA-5(5)	RA-5(5)	RA-5(5)	RA-5(5)	PRIVILEGED ACCESS
CA-1		CA-1	CA-1	CA-1	CA-1	CA-1	CA-1	CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
CA-2		CA-2					CA-2	CA-2	SECURITY ASSESSMENTS

Table 3 CECS Baseline Controls Breakdown, Part 3

			System Configuration						
			Interconnection Type						
	Controls Validated via Checklist		No IT Control System	Stand Alone Control System			COINv2 Interconnected Control System		
202	16	40	34	82	90	97	189	195	
Total Controls	ConMon Controls	ASR Core Controls	Low	Low	Moderate	High	Low	Moderate	Control Category/Family
CA-3		CA-3					CA-3	CA-3	SYSTEM INTERCONNECTIONS
CA-7		CA-7		CA-7	CA-7	CA-7	CA-7	CA-7	CONTINUOUS MONITORING
CA-7(1)							CA-7(1)	CA-7(1)	CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT
CA-9		CA-9		CA-9	CA-9	CA-9	CA-9	CA-9	INTERNAL SYSTEM CONNECTIONS
SC-1							SC-1	SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
SC-5							SC-5	SC-5	DENIAL-OF-SERVICE PROTECTION
SC-5(3)							SC-5(3)	SC-5(3)	DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING
SC-7		SC-7					SC-7	SC-7	BOUNDARY PROTECTION
SC-7(3)							SC-7(3)	SC-7(3)	BOUNDARY PROTECTION | ACCESS POINTS
SC-7(4)							SC-7(4)	SC-7(4)	BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES
SC-7(5)							SC-7(5)	SC-7(5)	BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION
SC-7(8)							SC-7(8)	SC-7(8)	BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS
SC-7(9)							SC-7(9)	SC-7(9)	BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC
SC-7(10)							SC-7(10)	SC-7(10)	BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION
SC-7(11)							SC-7(11)	SC-7(11)	BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC
SC-7(12)							SC-7(12)	SC-7(12)	BOUNDARY PROTECTION | HOST-BASED PROTECTION
SC-7(13)							SC-7(13)	SC-7(13)	BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS
SC-7(14)							SC-7(14)	SC-7(14)	BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTION
SC-7(18)						SC-7(18)			BOUNDARY PROTECTION | FAIL SECURE
SC-15							SC-15	SC-15	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS
SC-17							SC-17	SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES
SC-18							SC-18	SC-18	MOBILE CODE
SC-18(2)							SC-18(2)	SC-18(2)	MOBILE CODE | ACQUISITION / DEVELOPMENT / USE
SC-19							SC-19	SC-19	VOICE OVER INTERNET PROTOCOL
SC-22							SC-22	SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE
SC-23(5)							SC-23(5)	SC-23(5)	ALLOWED CERTIFICATE AUTHORITIES
SC-41						SC-41			PORT AND I/O DEVICE ACCESS
SI-1		SI-1	SI-1	SI-1	SI-1	SI-1	SI-1	SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
SI-2	SI-2			SI-2	SI-2	SI-2	SI-2	SI-2	FLAW REMEDIATION
SI-3							SI-3	SI-3	MALICIOUS CODE PROTECTION
SI-3(1)							SI-3(1)	SI-3(1)	MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT
SI-3(2)							SI-3(2)	SI-3(2)	MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES
SI-3(10)							SI-3(10)	SI-3(10)	MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS
SI-4	SI-4						SI-4	SI-4	SYSTEM MONITORING
SI-4(1)							SI-4(1)	SI-4(1)	INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM
SI-4(2)							SI-4(2)	SI-4(2)	INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS
SI-4(4)							SI-4(4)	SI-4(4)	INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC
SI-4(5)							SI-4(5)	SI-4(5)	INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS
SI-4(11)							SI-4(11)	SI-4(11)	INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES
SI-4(12)							SI-4(12)	SI-4(12)	INFORMATION SYSTEM MONITORING | AUTOMATED ALERTS
SI-4(16)							SI-4(16)	SI-4(16)	INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION
SI-4(19)							SI-4(19)	SI-4(19)	INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK
SI-4(20)							SI-4(20)	SI-4(20)	INFORMATION SYSTEM MONITORING | PRIVILEGED USER
SI-4(22)							SI-4(22)	SI-4(22)	INFORMATION SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES
SI-4(23)							SI-4(23)	SI-4(23)	INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES
SI-5							SI-5	SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
SI-7	SI-7				SI-7	SI-7		SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
SI-7(8)							SI-7(8)	SI-7(8)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS
SI-11				SI-11	SI-11	SI-11	SI-11	SI-11	ERROR HANDLING
SI-17						SI-17			FAIL-SAFE PROCEDURES
SA-1		SA-1	SA-1	SA-1	SA-1	SA-1	SA-1	SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
SA-3			SA-3	SA-3	SA-3	SA-3	SA-3	SA-3	SYSTEM DEVELOPMENT LIFE CYCLE
SA-4			SA-4	SA-4	SA-4	SA-4	SA-4	SA-4	ACQUISITION PROCESS
SA-4(10)							SA-4(10)	SA-4(10)	ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS
202	16	40	34	82	90	97	189	195	