ATTACHMENT

With reference to paragraph 15 of the Agreement, adequate security shall include, at minimum, implementation security and privacy controls in accordance with:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5* ("Rev 5"), *Security and Privacy Controls for Information Systems and Organizations*.

In September 2020, the National Institute of Standards and Technology (NIST), published an update, Revision 5, to NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organization*. SP 800-53 Revision 5 is part of the NIST Special Publication 800-series that reports on the NIST Information Technology Laboratory's (ITL) computer security-related research, guidelines, and outreach. The publication provides a comprehensive set of security controls, three security control baselines (low, moderate, and high impact), and guidance for tailoring the appropriate baseline to specific needs according to the organization's missions, environments of operation, and technologies used.

A separate guideline, SP 800-53B, *Control Baselines for Information Systems and Organizations*, provides specific guidelines that facilitate periodic assessment of security controls to ensure that controls have been implemented correctly, are operating as intended, and are meeting the organization's security requirements.

NIST SP 800-53 Rev 5 - Families

1. AC - Access Control (23)
2. AT - Awareness and Training (5)
3. AU - Audit and Accountability (15)
4. CA – Assessment, Authorization, and Monitoring (8)
5. CM - Configuration Management (14)
6. CP - Contingency Planning (12)
7. IA - Identification and Authentication (12)
8. IR - Incident Response (9)
9. MA – Maintenance (7)
10. MP - Media Protection (8)
11. PE - Physical and Environmental Protection (22)
12. PL – Planning (8)
13. PM – Program Management (32)
14. PS - Personnel Security (9)
15. PT – PII Processing and Transparency (8)
16. RA - Risk Assessment (9)
17. SA - System and Services Acquisition (16)
18. SC - System and Communications Protection (47)
19. SI - System and Information Integrity (22)
20. SR – Supply Chain Risk Management (12)

The 20 Families are broken into 322 Controls

(Note: There will be overlap in numbers between the baselines)

- 188 are High Impact
- 177 are Moderate Impact, and

- 131 are Low Impact

The following pages provide a breakdown of each control and the assigned impact level. Detailed requirements for each control can be found at: NIST Risk Management Framework | CSRC

Further understanding can be acquired from the NIST Special Publication 800-53, Rev 5, found at: http://csrc.nist.gov/publications/PubsSPs.html

No.	Control Name	Low-Impact	Moderate-Impact	High-Impact	Privacy Control Baseline
ACCESS CONTROL					
AC-1	POLICY AND PROCEDURES	AC-1	AC-1	AC-1	AC-1
AC-2	ACCOUNT MANAGEMENT	AC-2	AC-2 (1) (2) (3) (4) (5) (13)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)	
AC-3	ACCESS ENFORCEMENT	AC-3	AC-3	AC-3	AC-3 (14)
AC-4	INFORMATION FLOW ENFORCEMENT		AC-4	AC-4 (4)	
AC-5	SEPARATION OF DUTIES		AC-5	AC-5	
AC-6	LEAST PRIVILEGE		AC-6 (1) (2) (5) (7) (9) (10)	AC-6 (1) (2) (3) (5) (7) (9) (10)	
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	AC-7	AC-7	AC-7	
AC-8	SYSTEM USE NOTIFICATION	AC-8	AC-8	AC-8	
AC-9	PREVIOUS LOGON NOTIFICATION				
AC-10	CONCURRENT SESSION CONTROL			AC-10	

AC-11	DEVICE LOCK		AC-11 (1)	AC-11 (1)	
AC-12	SESSION TERMINATION		AC-12	AC-12	
AC-13	SUPERVISION AND REVIEW — ACCESS CONTROL				
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	AC-14	AC-14	AC-14	
AC-15	AUTOMATED MARKING				
AC-16	SECURITY AND PRIVACY ATTRIBUTES				
AC-17	REMOTE ACCESS	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)	
AC-18	WIRELESS ACCESS	AC-18	AC-18 (1) (3)	AC-18 (1) (3) (4) (5)	
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	AC-19	AC-19 (5)	AC-19 (5)	
AC-20	USE OF EXTERNAL SYSTEMS	AC-20	AC-20 (1) (2)	AC-20 (1) (2)	
AC-21	INFORMATION SHARING		AC-21	AC-21	
AC-22	PUBLICLY ACCESSIBLE CONTENT	AC-22	AC-22	AC-22	
AC-23	DATA MINING PROTECTION				
AC-24	ACCESS CONTROL DECISIONS				

AC-25	REFERENCE MONITOR				
AWARENESS AND TRAINING					
AT-1	POLICY AND PROCEDURES	AT-1	AT-1	AT-1	AT-1
AT-2	LITERACY TRAINING AND AWARENESS	AT-2 (2)	AT-2 (2) (3)	AT-2 (2) (3)	AT-2
AT-3	ROLE-BASED TRAINING	AT-3	AT-3	AT-3	AT-3 (5)
AT-4	TRAINING RECORDS	AT-4	AT-4	AT-4	AT-4
AT-5	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS				
AT-6	TRAINING FEEDBACK				
AUDIT AND ACCOUNTABILITY					
AU-1	POLICY AND PROCEDURES	AU-1	AU-1	AU-1	AU-1
AU-2	EVENT LOGGING	AU-2	AU-2	AU-2	AU-2
AU-3	CONTENT OF AUDIT RECORDS	AU-3	AU-3 (1)	AU-3 (1)	AU-3 (3)
AU-4	AUDIT LOG STORAGE CAPACITY	AU-4	AU-4	AU-4	
AU-5	RESPONSE TO AUDIT LOGGING PROCESS FAILURES	AU-5	AU-5	AU-5 (1) (2)	
AU-6	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)	

AU-7	AUDIT RECORD REDUCTION AND REPORT GENERATION		AU-7 (1)	AU-7 (1)	
AU-8	TIME STAMPS	AU-8	AU-8	AU-8	
AU-9	PROTECTION OF AUDIT INFORMATION	AU-9	AU-9 (4)	AU-9 (2) (3) (4)	
AU-10	NON-REPUDIATION			AU-10	
AU-11	AUDIT RECORD RETENTION	AU-11	AU-11	AU-11	AU-11
AU-12	AUDIT RECORD GENERATION	AU-12	AU-12	AU-12 (1) (3)	
AU-13	MONITORING FOR INFORMATION DISCLOSURE				
AU-14	SESSION AUDIT				
AU-15	ALTERNATE AUDIT LOGGING CAPABILITY				
AU-16	CROSS-ORGANIZATIONAL AUDIT LOGGING				
ASSESSMENT, AUTHORIZATION AND MONITORING					
CA-1	POLICY AND PROCEDURES	CA-1	CA-1	CA-1	CA-1
CA-2	CONTROL ASSESSMENTS	CA-2	CA-2 (1)	CA-2 (1) (2)	CA-2
CA-3	INFORMATION EXCHANGE	CA-3	CA-3	CA-3 (6)	

CA-4	SECURITY CERTIFICATION				
CA-5	PLAN OF ACTION AND MILESTONES	CA-5	CA-5	CA-5	CA-5
CA-6	AUTHORIZATION	CA-6	CA-6	CA-6	CA-6
CA-7	CONTINUOUS MONITORING	CA-7 (4)	CA-7 (1) (4)	CA-7 (1) (4)	CA-7 (4)
CA-8	PENETRATION TESTING			CA-8 (1)	
CA-9	INTERNAL SYSTEM CONNECTIONS	CA-9	CA-9	CA-9	
CONFIGURATION MANAGEMENT					
CM-1	POLICY AND PROCEDURES	CM-1	CM-1	CM-1	CM-1
CM-2	BASELINE CONFIGURATION	CM-2	CM-2 (2) (3) (7)	CM-2 (2) (3) (7)	
CM-3	CONFIGURATION CHANGE CONTROL		CM-3 (2) (4)	CM-3 (1) (2) (4) (6)	
CM-4	IMPACT ANALYSES	CM-4	CM-4 (2)	CM-4 (1) (2)	CM-4
CM-5	ACCESS RESTRICTIONS FOR CHANGE	CM-5	CM-5	CM-5 (1)	
CM-6	CONFIGURATION SETTINGS	CM-6	CM-6	CM-6 (1) (2)	
CM-7	LEAST FUNCTIONALITY	CM-7	CM-7 (1) (2) (5)	CM-7 (1) (2) (5)	
CM-8	SYSTEM COMPONENT INVENTORY	CM-8	CM-8 (1) (3)	CM-8 (1) (2) (3) (4)	

CM-9	CONFIGURATION MANAGEMENT PLAN		CM-9	CM-9	
CM-10	SOFTWARE USAGE RESTRICTIONS	CM-10	CM-10	CM-10	
CM-11	USER-INSTALLED SOFTWARE	CM-11	CM-11	CM-11	
CM-12	INFORMATION LOCATION		CM-12 (1)	CM-12 (1)	
CM-13	DATA ACTION MAPPING				
CM-14	SIGNED COMPONENTS				
CONTINGENCY PLANNING					
CP-1	POLICY AND PROCEDURES	CP-1	CP-1	CP-1	
CP-2	CONTINGENCY PLAN	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (5) (8)	
CP-3	CONTINGENCY TRAINING	CP-3	CP-3	CP-3 (1)	
CP-4	CONTINGENCY PLAN TESTING	CP-4	CP-4 (1)	CP-4 (1) (2)	
CP-5	CONTINGENCY PLAN UPDATE				
CP-6	ALTERNATE STORAGE SITE		CP-6 (1) (3)	CP-6 (1) (2) (3)	
CP-7	ALTERNATE PROCESSING SITE		CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)	
CP-8	TELECOMMUNICATIONS SERVICES		CP-8 (1) (2)	CP-8 (1) (2) (3) (4)	

CP-9	SYSTEM BACKUP	CP-9	CP-9 (1) (8)	CP-9 (1) (2) (3) (5) (8)	
CP-10	SYSTEM RECOVERY AND RECONSTITUTION	CP-10	CP-10 (2)	CP-10 (2) (4)	
CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS				
CP-12	SAFE MODE				
CP-13	ALTERNATIVE SECURITY MECHANISMS				
IDENTIFICATION AND AUTHENTICATION					
IA-1	POLICY AND PROCEDURES	IA-1	IA-1	IA-1	
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	IA-2 (1) (2) (8) (12)	IA-2 (1) (2) (8) (12)	IA-2 (1) (2) (5) (8) (12)	
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION		IA-3	IA-3	
IA-4	IDENTIFIER MANAGEMENT	IA-4	IA-4 (4)	IA-4 (4)	
IA-5	AUTHENTICATOR MANAGEMENT	IA-5 (1)	IA-5 (1) (2) (6)	IA-5 (1) (2) (6)	
IA-6	AUTHENTICATION FEEDBACK	IA-6	IA-6	IA-6	
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	IA-7	IA-7	IA-7	
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-	IA-8 (1) (2) (4)	IA-8 (1) (2) (4)	IA-8 (1) (2) (4)	

	ORGANIZATIONAL USERS)				
IA-9	SERVICE IDENTIFICATION AND AUTHENTICATION				
IA-10	ADAPTIVE AUTHENTICATION				
IA-11	RE-AUTHENTICATION	IA-11	IA-11	IA-11	
IA-12	IDENTITY PROOFING		IA-12 (2) (3) (5)	IA-12 (2) (3) (4) (5)	
INCIDENT RESPONSE					
IR-1	POLICY AND PROCEDURES	IR-1	IR-1	IR-1	IR-1
IR-2	INCIDENT RESPONSE TRAINING	IR-2	IR-2	IR-2 (1) (2)	IR-2 (3)
IR-3	INCIDENT RESPONSE TESTING		IR-3 (2)	IR-3 (2)	IR-3
IR-4	INCIDENT HANDLING	IR-4	IR-4 (1)	IR-4 (1) (4) (11)	IR-4
IR-5	INCIDENT MONITORING	IR-5	IR-5	IR-5 (1)	IR-5
IR-6	INCIDENT REPORTING	IR-6	IR-6 (1) (3)	IR-6 (1) (3)	IR-6
IR-7	INCIDENT RESPONSE ASSISTANCE	IR-7	IR-7 (1)	IR-7 (1)	IR-7
IR-8	INCIDENT RESPONSE PLAN	IR-8	IR-8	IR-8	IR-8 (1)
IR-9	INFORMATION SPILLAGE RESPONSE				

IR-10	INTEGRATED INFORMATION SECURITY ANALYSIS TEAM				
MAINTENANCE					
MA-1	POLICY AND PROCEDURES	MA-1	MA-1	MA-1	
MA-2	CONTROLLED MAINTENANCE	MA-2	MA-2	MA-2 (2)	
MA-3	MAINTENANCE TOOLS		MA-3 (1) (2) (3)	MA-3 (1) (2) (3)	
MA-4	NONLOCAL MAINTENANCE	MA-4	MA-4	MA-4 (3)	
MA-5	MAINTENANCE PERSONNEL	MA-5	MA-5	MA-5 (1)	
MA-6	TIMELY MAINTENANCE		MA-6	MA-6	
MA-7	FIELD MAINTENANCE				
MEDIA PROTECTION					
MP-1	POLICY AND PROCEDURES	MP-1	MP-1	MP-1	MP-1
MP-2	MEDIA ACCESS	MP-2	MP-2	MP-2	
MP-3	MEDIA MARKING		MP-3	MP-3	
MP-4	MEDIA STORAGE		MP-4	MP-4	
MP-5	MEDIA TRANSPORT		MP-5	MP-5	
MP-6	MEDIA SANITIZATION	MP-6	MP-6	MP-6 (1) (2) (3)	MP-6

MP-7	MEDIA USE	MP-7	MP-7	MP-7	
MP-8	MEDIA DOWNGRADING				
PHYSICAL AND ENVIRONMENTAL PROTECTION					
PE-1	POLICY AND PROCEDURES	PE-1	PE-1	PE-1	
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	PE-2	PE-2	PE-2	
PE-3	PHYSICAL ACCESS CONTROL	PE-3	PE-3	PE-3 (1)	
PE-4	ACCESS CONTROL FOR TRANSMISSION		PE-4	PE-4	
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES		PE-5	PE-5	
PE-6	MONITORING PHYSICAL ACCESS	PE-6	PE-6 (1)	PE-6 (1) (4)	
PE-7	VISITOR CONTROL				
PE-8	VISITOR ACCESS RECORDS	PE-8	PE-8	PE-8 (1)	PE-8 (3)
PE-9	POWER EQUIPMENT AND CABLING		PE-9	PE-9	
PE-10	EMERGENCY SHUTOFF		PE-10	PE-10	
PE-11	EMERGENCY POWER		PE-11	PE-11 (1)	
PE-12	EMERGENCY LIGHTING	PE-12	PE-12	PE-12	

PE-13	FIRE PROTECTION	PE-13	PE-13 (1)	PE-13 (1) (2)	
PE-14	ENVIRONMENTAL CONTROLS	PE-14	PE-14	PE-14	
PE-15	WATER DAMAGE PROTECTION	PE-15	PE-15	PE-15 (1)	
PE-16	DELIVERY AND REMOVAL	PE-16	PE-16	PE-16	
PE-17	ALTERNATE WORK SITE		PE-17	PE-17	
PE-18	LOCATION OF SYSTEM COMPONENTS			PE-18	
PE-19	INFORMATION LEAKAGE				
PE-20	ASSET MONITORING AND TRACKING				
PE-21	ELECTROMAGNETIC PULSE PROTECTION				
PE-22	COMPONENT MARKING				
PE-23	FACILITY LOCATION				
PLANNING					
PL-1	POLICY AND PROCEDURES	PL-1	PL-1	PL-1	PL-1
PL-2	SYSTEM SECURITY AND PRIVACY PLANS	PL-2	PL-2	PL-2	PL-2
PL-3	SYSTEM SECURITY PLAN UPDATE				
PL-4	RULES OF BEHAVIOR	PL-4 (1)	PL-4 (1)	PL-4 (1)	PL-4 (1)

PL-5	PRIVACY IMPACT ASSESSMENT				
PL-6	SECURITY-RELATED ACTIVITY PLANNING				
PL-7	CONCEPT OF OPERATIONS				
PL-8	SECURITY AND PRIVACY ARCHITECTURES		PL-8	PL-8	PL-8
PL-9	CENTRAL MANAGEMENT				PL-9
PL-10	BASELINE SELECTION	PL-10	PL-10	PL-10	
PL-11	BASELINE TAILORING	PL-11	PL-11	PL-11	
PROGRAM MANAGEMENT					
PM-1	INFORMATION SECURITY PROGRAM PLAN				
PM-2	INFORMATION SECURITY PROGRAM LEADERSHIP ROLE				
PM-3	INFORMATION SECURITY AND PRIVACY RESOURCES				PM-3
PM-4	PLAN OF ACTION AND MILESTONES PROCESS				PM-4
PM-5	SYSTEM INVENTORY				PM-5 (1)
PM-6	MEASURES OF				PM-6

	PERFORMANCE				
PM-7	ENTERPRISE ARCHITECTURE				PM-7
PM-8	CRITICAL INFRASTRUCTURE PLAN				PM-8
PM-9	RISK MANAGEMENT STRATEGY				PM-9
PM-10	AUTHORIZATION PROCESS				PM-10
PM-11	MISSION AND BUSINESS PROCESS DEFINITION				PM-11
PM-12	INSIDER THREAT PROGRAM				
PM-13	SECURITY AND PRIVACY WORKFORCE				PM-13
PM-14	TESTING, TRAINING, AND MONITORING				PM-14
PM-15	SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS				
PM-16	THREAT AWARENESS PROGRAM				
PM-17	PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS				PM-17
PM-18	PRIVACY PROGRAM PLAN				PM-18

PM-19	PRIVACY PROGRAM LEADERSHIP ROLE				PM-19
PM-20	DISSEMINATION OF PRIVACY PROGRAM INFORMATION				PM-20 (1)
PM-21	ACCOUNTING OF DISCLOSURES				PM-21
PM-22	PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT				PM-22
PM-23	DATA GOVERNANCE BODY				
PM-24	DATA INTEGRITY BOARD				PM-24
PM-25	MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH				PM-25
PM-26	COMPLAINT MANAGEMENT				PM-26
PM-27	PRIVACY REPORTING				PM-27
PM-28	RISK FRAMING				PM-28
PM-29	RISK MANAGEMENT PROGRAM LEADERSHIP ROLES				
PM-30	SUPPLY CHAIN RISK MANAGEMENT STRATEGY				

PM-31	CONTINUOUS MONITORING STRATEGY				PM-31
PM-32	PURPOSING				
PERSONNEL SECURITY					
PS-1	POLICY AND PROCEDURES	PS-1	PS-1	PS-1	
PS-2	POSITION RISK DESIGNATION	PS-2	PS-2	PS-2	
PS-3	PERSONNEL SCREENING	PS-3	PS-3	PS-3	
PS-4	PERSONNEL TERMINATION	PS-4	PS-4	PS-4 (2)	
PS-5	PERSONNEL TRANSFER	PS-5	PS-5	PS-5	
PS-6	ACCESS AGREEMENTS	PS-6	PS-6	PS-6	PS-6
PS-7	EXTERNAL PERSONNEL SECURITY	PS-7	PS-7	PS-7	
PS-8	PERSONNEL SANCTIONS	PS-8	PS-8	PS-8	
PS-9	POSITION DESCRIPTIONS	PS-9	PS-9	PS-9	
PII PROCESSING AND TRANSPARENCY					
PT-1	POLICY AND PROCEDURES				PT-1
PT-2	AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION				PT-2

PT-3	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES				PT-3
PT-4	CONSENT				PT-4
PT-5	PRIVACY NOTICE				PT-5 (2)
PT-6	SYSTEM OF RECORDS NOTICE				PT-6 (1) (2)
PT-7	SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION				PT-7 (1) (2)
PT-8	COMPUTER MATCHING REQUIREMENTS				PT-8
RISK ASSESSMENT					
RA-1	POLICY AND PROCEDURES	RA-1	RA-1	RA-1	RA-1
RA-2	SECURITY CATEGORIZATION	RA-2	RA-2	RA-2	
RA-3	RISK ASSESSMENT	RA-3 (1)	RA-3 (1)	RA-3 (1)	RA-3
RA-4	RISK ASSESSMENT UPDATE				
RA-5	VULNERABILITY MONITORING AND SCANNING	RA-5 (2) (11)	RA-5 (2) (5) (11)	RA-5 (2) (4) (5) (11)	
RA-6	TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY				

RA-7	RISK RESPONSE	RA-7	RA-7	RA-7	RA-7
RA-8	PRIVACY IMPACT ASSESSMENTS				RA-8
RA-9	CRITICALITY ANALYSIS		RA-9	RA-9	
RA-10	THREAT HUNTING				
SYSTEM AND SERVICES AQUISITION					
SA-1	POLICY AND PROCEDURES	SA-1	SA-1	SA-1	SA-1
SA-2	ALLOCATION OF RESOURCES	SA-2	SA-2	SA-2	SA-2
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	SA-3	SA-3	SA-3	SA-3
SA-4	ACQUISITION PROCESS	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (5) (9) (10)	SA-4
SA-5	SYSTEM DOCUMENTATION	SA-5	SA-5	SA-5	
SA-6	SOFTWARE USAGE RESTRICTIONS				
SA-7	USER-INSTALLED SOFTWARE				
SA-8	SECURITY AND PRIVACY ENGINEERING PRINCIPLES	SA-8	SA-8	SA-8	SA-8 (33)
SA-9	EXTERNAL SYSTEM SERVICES	SA-9	SA-9 (2)	SA-9 (2)	SA-9

SA-10	DEVELOPER CONFIGURATION MANAGEMENT		SA-10	SA-10	
SA-11	DEVELOPER TESTING AND EVALUATION		SA-11	SA-11	SA-11
SA-12	SUPPLY CHAIN PROTECTION				
SA-13	TRUSTWORTHINESS				
SA-14	CRITICALITY ANALYSIS				
SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS		SA-15 (3)	SA-15 (3)	
SA-16	DEVELOPER-PROVIDED TRAINING			SA-16	
SA-17	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN			SA-17	
SA-18	TAMPER RESISTANCE AND DETECTION				
SA-19	COMPONENT AUTHENTICITY				
SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS				
SA-21	DEVELOPER SCREENING			SA-21	
SA-22	UNSUPPORTED SYSTEM COMPONENTS	SA-22	SA-22	SA-22	

SA-23	SPECIALIZATION				
SYSTEM AND COMMUNICATIONS PROTECTION					
SC-1	POLICY AND PROCEDURES	SC-1	SC-1	SC-1	
SC-2	SEPARATION OF SYSTEM AND USER FUNCTIONALITY		SC-2	SC-2	
SC-3	SECURITY FUNCTION ISOLATION			SC-3	
SC-4	INFORMATION IN SHARED SYSTEM RESOURCES		SC-4	SC-4	
SC-5	DENIAL-OF-SERVICE PROTECTION	SC-5	SC-5	SC-5	
SC-6	RESOURCE AVAILABILITY				
SC-7	BOUNDARY PROTECTION	SC-7	SC-7 (3) (4) (5) (7) (8)	SC-7 (3) (4) (5) (7) (8) (18) (21)	SC-7 (24)
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY		SC-8 (1)	SC-8 (1)	
SC-9	TRANSMISSION CONFIDENTIALITY				
SC-10	NETWORK DISCONNECT		SC-10	SC-10	
SC-11	TRUSTED PATH				
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC-12	SC-12	SC-12 (1)	

SC-13	CRYPTOGRAPHIC PROTECTION	SC-13	SC-13	SC-13	
SC-14	PUBLIC ACCESS PROTECTIONS				
SC-15	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS	SC-15	SC-15	SC-15	
SC-16	TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES				
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES		SC-17	SC-17	
SC-18	MOBILE CODE		SC-18	SC-18	
SC-19	VOICE OVER INTERNET PROTOCOL				
SC-20	SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	SC-20	SC-20	SC-20	
SC-21	SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	SC-21	SC-21	SC-21	
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE	SC-22	SC-22	SC-22	
SC-23	SESSION AUTHENTICITY		SC-23	SC-23	
SC-24	FAIL IN KNOWN STATE			SC-24	

SC-25	THIN NODES				
SC-26	DECOYS				
SC-27	PLATFORM-INDEPENDENT APPLICATIONS				
SC-28	PROTECTION OF INFORMATION AT REST		SC-28 (1)	SC-28 (1)	
SC-29	HETEROGENEITY				
SC-30	CONCEALMENT AND MISDIRECTION				
SC-31	COVERT CHANNEL ANALYSIS				
SC-32	SYSTEM PARTITIONING				
SC-33	TRANSMISSION PREPARATION INTEGRITY				
SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS				
SC-35	EXTERNAL MALICIOUS CODE IDENTIFICATION				
SC-36	DISTRIBUTED PROCESSING AND STORAGE				
SC-37	OUT-OF-BAND CHANNELS				
SC-38	OPERATIONS SECURITY				
SC-39	PROCESS ISOLATION	SC-39	SC-39	SC-39	

SC-40	WIRELESS LINK PROTECTION				
SC-41	PORT AND I/O DEVICE ACCESS				
SC-42	SENSOR CAPABILITY AND DATA				
SC-43	USAGE RESTRICTIONS				
SC-44	DETONATION CHAMBERS				
SC-45	SYSTEM TIME SYNCHRONIZATION				
SC-46	CROSS DOMAIN POLICY ENFORCEMENT				
SC-47	ALTERNATE COMMUNICATIONS PATHS				
SC-48	SENSOR RELOCATION				
SC-49	HARDWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT				
SC-50	SOFTWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT				
SC-51	HARDWARE-BASED PROTECTION				
SYSTEM AND INFORMATION INTEGRITY					
SI-1	POLICY AND PROCEDURES	SI-1	SI-1	SI-1	SI-1

SI-2	FLAW REMEDIATION	SI-2	SI-2 (2)	SI-2 (2)	
SI-3	MALICIOUS CODE PROTECTION	SI-3	SI-3	SI-3	
SI-4	SYSTEM MONITORING	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5) (10) (12) (14) (20) (22)	
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	SI-5	SI-5	SI-5 (1)	
SI-6	SECURITY AND PRIVACY FUNCTION VERIFICATION			SI-6	
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY		SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (15)	
SI-8	SPAM PROTECTION		SI-8 (2)	SI-8 (2)	
SI-9	INFORMATION INPUT RESTRICTIONS				
SI-10	INFORMATION INPUT VALIDATION		SI-10	SI-10	
SI-11	ERROR HANDLING		SI-11	SI-11	
SI-12	INFORMATION MANAGEMENT AND RETENTION	SI-12	SI-12	SI-12	SI-12 (1) (2) (3)
SI-13	PREDICTABLE FAILURE PREVENTION				
SI-14	NON-PERSISTENCE				
SI-15	INFORMATION OUTPUT FILTERING				

SI-16	MEMORY PROTECTION		SI-16	SI-16	
SI-17	FAIL-SAFE PROCEDURES				
SI-18	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS				SI-18 (4)
SI-19	DE-IDENTIFICATION				SI-19
SI-20	TAINTING				
SI-21	INFORMATION REFRESH				
SI-22	INFORMATION DIVERSITY				
SI-23	INFORMATION FRAGMENTATION				
SUPPLY CHAIN RISK MANAGEMENT					
SR-1	POLICY AND PROCEDURES	SR-1	SR-1	SR-1	
SR-2	SUPPLY CHAIN RISK MANAGEMENT PLAN	SR-2 (1)	SR-2 (1)	SR-2 (1)	
SR-3	SUPPLY CHAIN CONTROLS AND PROCESSES	SR-3	SR-3	SR-3	
SR-4	PROVENANCE				
SR-5	ACQUISITION STRATEGIES, TOOLS, AND METHODS	SR-5	SR-5	SR-5	
SR-6	SUPPLIER ASSESSMENTS AND REVIEWS		SR-6	SR-6	

SR-7	SUPPLY CHAIN OPERATIONS SECURITY				
SR-8	NOTIFICATION AGREEMENTS	SR-8	SR-8	SR-8	
SR-9	TAMPER RESISTANCE AND DETECTION			SR-9 (1)	
SR-10	INSPECTION OF SYSTEMS OR COMPONENTS	SR-10	SR-10	SR-10	
SR-11	COMPONENT AUTHENTICITY	SR-11 (1) (2)	SR-11 (1) (2)	SR-11 (1) (2)	
SR-12	COMPONENT DISPOSAL	SR-12	SR-12	SR-12	