APPENDIX D

CONTROL BASELINES

TABLE D-1: CONTROL BASELINES

CNTL NO.	CONTROL NAME	PRIVACY-RELATED	CONTROL BASELINES		
			LOW	MODERATE	HIGH
	Access Control – AC				
AC-1	Access Control Policy and Procedures		AC-1	AC-1	AC-1
AC-2	Account Management		AC-2	AC-2 (1) (2) (3) (4) (5) (10) (13)	AC-2 (1) (2) (3) (4) (5) (10) (11) (12) (13)
AC-3	Access Enforcement		AC-3	AC-3	AC-3
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 (7) (9)~~—~~	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 (Access) 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AC-13	Withdrawn				
AC-14	Permitted Actions without Identification or Authentication		AC-14	AC-14	AC-14
AC-15	Withdrawn				
AC-16	Security and Privacy Attributes	P	—	—	—
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)	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	P	—	AC-21	AC-21
AC-22	Publicly Accessible Content		AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P	—	—	—
AC-24	Access Control Decisions		—	—	—
AC-25	Reference Monitor		—	—	—
	Awareness and Training – AT				
AT-1	~~Security~~ Awareness and Training Policy and Procedures	P	AT-1	AT-1	AT-1

Commented [A1]: Please note that this column, "Privacy-Related" is new to Rev. 5. All content in this column is also new.

In Rev.4, there was a column titled, "Priority" that was removed.

CNTL NO.	CONTROL NAME	PRIVACY-RELATED	CONTROL BASELINES		
			LOW	MODERATE	HIGH
AT-2	Awareness Training	P	AT-2	AT-2 (2) (3)	AT-2 (2) (3)
AT-3	Role-Based ~~Security~~ Training	P	AT-3	AT-3	AT-3
AT-4	~~Security~~ Training Records	P	AT-4	AT-4	AT-4
AT-5	Withdrawn				
Audit and Accountability – AU					
AU-1	Audit and Accountability Policy and Procedures		AU-1	AU-1	AU-1
AU-2	Audit Events		AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records		AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity		AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures		AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting		AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Audit Reduction and Report Generation		—	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps		AU-8	AU-8 (1)	AU-8 (1)
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	P	AU-11	AU-11	AU-11
AU-12	Audit Generation		AU-12	AU-12	AU-12 (1) (3)
AU-13	Monitoring for Information Disclosure		—	—	—
AU-14	Session Audit		—	—	—
AU-15	Alternate Audit Capability		—	—	—
AU-16	Cross-Organizational Auditing	P	—	—	—
Assessment and Authorization – CA					
CA-1	~~Security~~ Assessment and Authorization Policy and Procedures	P	CA-1	CA-1	CA-1
CA-2	~~Security~~ Assessments	P	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections		CA-3	CA-3 (5)	CA-3 (5) (6)
CA-4	Withdrawn				
CA-5	Plan of Action and Milestones	P	CA-5	CA-5	CA-5
CA-6	~~Security~~ Authorization		CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P	CA-7 (4)	CA-7 (1) (4)	CA-7 (1) (4)
CA-8	Penetration Testing		—	—	CA-8 (1)
CA-9	Internal System Connections		CA-9	CA-9	CA-9
Configuration Management – CM					
CM-1	Configuration Management Policy and Procedures	P	CM-1	CM-1	CM-1
CM-2	Baseline Configuration		CM-2	CM-2 ~~(1)~~ (2) (3) (7)	CM-2 ~~(1)~~ (2) (3) (7)

Commented [A1]: Please note that this column, "Privacy-Related" is new to Rev. 5. All content in this column is also new.

In Rev.4, there was a column titled, "Priority" that was removed.

CNTL NO.	CONTROL NAME	PRIVACY-RELATED	CONTROL BASELINES		
			LOW	MODERATE	HIGH
CM-3	Configuration Change Control		—	CM-3 (2) (4)	CM-3 (1) (2) (4) (6)
CM-4	Security and Privacy Impact Analyses	P	CM-4	CM-4 (2)	CM-4 (1) (2)
CM-5	Access Restrictions for Change		CM-5~~Not Selected~~	CM-5	CM-5 (1) (2) (3)
CM-6	Configuration Settings		CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality		CM-7	CM-7 (1) (2) (5~~4~~)	CM-7 (1) (2) (5)
CM-8	System Component Inventory		CM-8	CM-8 (1) (3) ~~(5)~~	CM-8 (1) (2) (3) (4) ~~(5)~~
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	P	—	CM-12 (1)	CM-12 (1)
Contingency Planning – CP					
CP-1	Contingency Planning Policy and Procedures	P	CP-1	CP-1	CP-1
CP-2	Contingency Plan	P	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	P	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	P	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	Withdrawn				
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					
IA-1	Identification and Authentication Policy and Procedures	P	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)		IA-2 (1) (2) (8) (12)	IA-2 (1) (2) (3) (8) ~~(11)~~ (12)	IA-2 (1) (2) (3) (4) (8) ~~(9) (11)~~ (12)
IA-3	Device Identification and Authentication		—	IA-3	IA-3
IA-4	Identifier Management	P	IA-4	IA-4 (4)	IA-4 (4)

Commented [A1]: Please note that this column, "Privacy-Related" is new to Rev. 5. All content in this column is also new.

In Rev.4, there was a column titled, "Priority" that was removed.

CNTL NO.	CONTROL NAME	PRIVACY-RELATED	CONTROL BASELINES		
			LOW	MODERATE	HIGH
IA-5	Authenticator Management		IA-5 (1) (11)	IA-5 (1) (2) ~~(3)~~ (6) ~~(11)~~	IA-5 (1) (2) ~~(3)~~ (6) ~~(11)~~
IA-6	Authenticator Feedback		IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication		IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P	IA-8 (1) (2) ~~(3)~~ (4)	IA-8 (1) (2) ~~(3)~~ (4)	IA-8 (1) (2) ~~(3)~~ (4)
IA-9	Service Identification and Authentication		—	—	—
IA-10	Adaptive Identification and 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)
Individual Participation – IP					
IP-1	Individual Participation Policy and Procedures	P	Privacy-related controls and enhancements are not allocated to baselines in this table. See Appendix F for control selection and implementation guidance.		
IP-2	Consent	P			
IP-3	Redress	P			
IP-4	Privacy Notice	P			
IP-5	Privacy Act Statement	P			
IP-6	Individual Access	P			
Incident Response – IR					
IR-1	Incident Response Policy and Procedures	P	IR-1	IR-1	IR-1
IR-2	Incident Response Training	P	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing	P	—	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	P	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	Incident Monitoring	P	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	P	IR-6	IR-6 (1) (3)	IR-6 (1) (3)
IR-7	Incident Response Assistance	P	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	P	IR-8	IR-8	IR-8
IR-9	Information Spillage Response	P	—	—	—
IR-10	Integrated Information Security Analysis Team		—	—	IR-10~~Not Selected~~
Maintenance – MA					
MA-1	System Maintenance 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 ~~(2)~~	MA-4 ~~(2)~~ (3)
MA-5	Maintenance Personnel		MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance		—	MA-6	MA-6

Commented [A1]: Please note that this column, “Privacy-Related” is new to Rev. 5. All content in this column is also new.

In Rev.4, there was a column titled, “Priority” that was removed.

CNTL NO.	CONTROL NAME	PRIVACY-RELATED	CONTROL BASELINES		
			LOW	MODERATE	HIGH
Media Protection – MP					
MP-1	Media Protection Policy and Procedures		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 ~~(4)~~	MP-5 ~~(4)~~
MP-6	Media Sanitization		MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	Media Use		MP-7	MP-7 ~~(1)~~	MP-7 ~~(1)~~
MP-8	Media Downgrading		—	—	—
Privacy Authorization – PA					
PA-1	Privacy Authorization Policy and Procedures	P	Privacy-related controls and enhancements are not allocated to baselines in this table. See **Appendix F** for control selection and implementation guidance.		
PA-2	Authority to Collect	P			
PA-3	Purpose Specification	P			
PA-4	Information Sharing with External Parties	P			
Physical and Environmental Protection – PE					
PE-1	Physical and Environmental Protection 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 ~~Medium~~		—	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	Withdrawn				
PE-8	Visitor Access Records		PE-8	PE-8	PE-8 (1)
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 ~~(3)~~ (1) (2)	PE-13 (1) (2) ~~(3)~~
PE-14	Temperature and Humidity 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 ~~Information~~ System Components		—	—	PE-18
PE-19	Information Leakage		—	—	—
PE-20	Asset Monitoring and Tracking		—	—	—
PE-21	Electromagnetic Pulse Protection		—	—	—
PE-22	Component Marking		—	—	—

Commented [A1]: Please note that this column, "Privacy-Related" is new to Rev. 5. All content in this column is also new.

In Rev.4, there was a column titled, "Priority" that was removed.

CNTL NO.	CONTROL NAME	PRIVACY-RELATED	CONTROL BASELINES		
			LOW	MODERATE	HIGH
Planning – PL					
PL-1	~~Security~~ Planning Policy and Procedures	P	PL-1	PL-1	PL-1
PL-2	System Security and Privacy Plans	P	PL-2	PL-2 (3)	PL-2 (3)
PL-3	Withdrawn				
PL-4	Rules of Behavior	P	PL-4	PL-4 (1)	PL-4 (1)
PL-5	Withdrawn				
PL-6	Withdrawn				
PL-7	~~Security~~ Concept of Operations	P	—	—	—
PL-8	~~Information~~ Security and Privacy Architectures~~s~~	P	—	PL-8	PL-8
PL-9	Central Management	P	—	—	—
PL-10	Baseline Selection		PL-10	PL-10	PL-10
PL-11	Baseline Tailoring		PL-11	PL-11	PL-11
Program Management – PM					
PM-1	Information Security Program Plan		~~Deployed organization-wide. Supporting information security program. Not associated with security control baselines. Independent of any system impact level.~~ Security and privacy controls in the **PM family** have been designed to facilitate compliance with laws, Executive Orders, directives, regulations, policies, and standards. PM controls are independent of any FIPS 200 impact levels and are not directly associated with the control baselines in **Appendix D**. Tailoring guidance can also be applied to the controls. See **Appendix G**. PM controls focus on the programmatic, organization-wide security and privacy requirements independent of any system and essential for managing security and privacy programs. Organizations can document the controls in their information security and privacy program plans. These		
PM-2	~~Senior Information Security Officer~~ Information Security Program Roles				
PM-3	Information Security and Privacy Resources	P			
PM-4	Plan of Action and Milestones Process	P			
PM-5	~~Information~~ System Inventory				
PM-6	~~Information Security Information Security~~ Measures of Performance	P			
PM-7	Enterprise Architecture	P			
PM-8	Critical Infrastructure Plan	P			
PM-9	Risk Management Strategy	P			
PM-10	~~Security~~ Authorization Process				
PM-11	Mission and Business Process Definition	P			
PM-12	Insider Threat Program				
PM-13	~~Information~~ Security and Privacy Workforce	P			
PM-14	Testing, Training, and Monitoring	P			
PM-15	Contacts with ~~Security~~ Groups and Associations	P			
PM-16	Threat Awareness Program				
PM-17	External Authorization				
PM-18	Privacy Program Plan	P			
PM-19	Senior Agency Official for Privacy	P			
PM-20	System of Records Notice	P			
PM-21	Dissemination of Privacy Program Information	P			

Commented [A1]: Please note that this column, "Privacy-Related" is new to Rev. 5. All content in this column is also new.

In Rev.4, there was a column titled, "Priority" that was removed.

Commented [A2]: Please note that the Program Management control family was in a separate Appendix in Rev.4.

CNTL NO.	CONTROL NAME	PRIVACY-RELATED	CONTROL BASELINES		
			LOW	MODERATE	HIGH
PM-22	Accounting of Disclosures	P	plans, together with the security and privacy plans for the individual systems, cover the totality of security and privacy controls that are employed by the organization. Privacy-related controls and control enhancements are not allocated to baselines in this table. See **Appendix F** for control selection and implementation guidance.~~Organization-wide Common ControlOrganization-wide Common Contr~~		
PM-23	Data Quality Management	P			
PM-24	Data Management Board	P			
PM-25	Data Integrity Board	P			
PM-26	Minimization of Personally Identifiable Information	P			
PM-27	Individual Access Control	P			
PM-28	Complaint Management	P			
PM-29	Inventory of Personally Identifiable Information	P			
PM-30	Privacy Reporting	P			
PM-31	Supply Chain Risk Management Plan				
PM-32	Risk Framing				
Personnel Security – PS					
PS-1	Personnel Security 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-7	External ~~Third-Party~~ Personnel Security		PS-7	PS-7	PS-7
PS-8	Personnel Sanctions		PS-8	PS-8	PS-8
Risk Assessment – RA					
RA-1	Risk Assessment Policy and Procedures	P	RA-1	RA-1	RA-1
RA-2	Security Categorization		RA-2	RA-2	RA-2
RA-3	Risk Assessment	P	RA-3	RA-3 (1)	RA-3 (1)
RA-4	**Withdrawn**				
RA-5	Vulnerability Scanning		RA-5 (2)	RA-5 ~~(1)~~ (2) (5)	RA-5 ~~(1)~~ (2) (4) (5)
RA-6	Technical Surveillance Countermeasures Survey		—	—	—
RA-7	Risk Response	P	RA-7	RA-7	RA-7
RA-8	Privacy Impact Assessment	P	—	—	—
RA-9	Criticality Analysis		—	RA-9~~—~~	RA-9
System and Services Acquisition – SA					
SA-1	System and Services Acquisition Policy and Procedures	P	SA-1	SA-1	SA-1
SA-2	Allocation of Resources		SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	P	SA-3	SA-3	SA-3

Commented [A1]: Please note that this column, “Privacy-Related” is new to Rev. 5. All content in this column is also new.

In Rev.4, there was a column titled, “Priority” that was removed.

CNTL NO.	CONTROL NAME	PRIVACY-RELATED	CONTROL BASELINES		
			LOW	MODERATE	HIGH
SA-4	Acquisition Process	P	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (5) (9) (10)
SA-5	~~Information~~ System Documentation		SA-5	SA-5	SA-5
SA-6	Withdrawn				
SA-7	Withdrawn				
SA-8	Security and Privacy Engineering Principles	P	SA-8~~Not Selected~~	SA-8	SA-8
SA-9	External ~~Information~~ System Services	P	SA-9	SA-9 (2)	SA-9 (2)
SA-10	Developer Configuration Management		—	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P	—	SA-11	SA-11
SA-12	Supply Chain Risk Management~~Protection~~		—	SA-12~~Not Selected~~	SA-12 (2) (10) (16)
SA-13	Withdrawn	~~Not Selected~~			
SA-14	Withdrawn				
SA-15	Development Process, Standards, and Tools		—	SA-15 (3)~~—~~	SA-15 (3)
SA-16	Developer-Provided Training		—	—	SA-16
SA-17	Developer Security 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~~Not Selected~~
SA-22	Unsupported System Components		SA-22~~Not Selected~~	SA-22~~Not Selected~~	SA-22~~Not Selected~~
System and Communications Protection – SC					
SC-1	System and Communications Protection Policy and Procedures	P	SC-1	SC-1	SC-1
SC-2	Application Partitioning		—	SC-2	SC-2
SC-3	Security Function Isolation		—	—	SC-3
SC-4	Information in Shared Systems 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-8	Transmission Confidentiality and Integrity		—	SC-8 (1)	SC-8 (1)
SC-9	Withdrawn				

Commented [A1]: Please note that this column, "Privacy-Related" is new to Rev. 5. All content in this column is also new.

In Rev.4, there was a column titled, "Priority" that was removed.

CNTL NO.	CONTROL NAME	PRIVACY-RELATED	CONTROL BASELINES		
			LOW	MODERATE	HIGH
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	Withdrawn				
SC-15	Collaborative Computing Devices and Applications		SC-15	SC-15	SC-15
SC-16	Transmission of Security and Privacy Attributes	P	—	—	—
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-19	SC-19
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	Honeypots		—	—	—
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	~~Information~~ System Partitioning		—	—	—
SC-33	Withdrawn				
SC-34	Non-Modifiable Executable Programs		—	—	—
SC-35	Honeyclients		—	—	—
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	P	—	—	—
SC-43	Usage Restrictions		—	—	—
SC-44	Detonation Chambers		—	—	—

System and Information Integrity – SI

Commented [A1]: Please note that this column, “Privacy-Related” is new to Rev. 5. All content in this column is also new.

In Rev.4, there was a column titled, “Priority” that was removed.

CNTL NO.	CONTROL NAME	PRIVACY-RELATED	CONTROL BASELINES		
			LOW	MODERATE	HIGH
SI-1	System and Information Integrity Policy and Procedures	P	SI-1	SI-1	SI-1
SI-2	Flaw Remediation		SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection		SI-3	SI-3 (1) ~~(2)~~	SI-3 (1) ~~(2)~~
SI-4	~~Information~~ 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	P	—	—	SI-6
SI-7	Software, Firmware, and Information Integrity		—	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14) (15)
SI-8	Spam Protection		—	SI-8 (1) (2)	SI-8 (1) (2)
SI-9	Withdrawn				
SI-10	Information Input Validation		—	SI-10	SI-10
SI-11	Error Handling		—	SI-11	SI-11
SI-12	Information Management~~Handling~~ and Retention	P	SI-12	SI-12	SI-12
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	Information Disposal	P	—	—	—
SI-19	Data Quality Operations	P	—	—	—
SI-20	De-Identification	P	—	—	—
Note: Privacy-related controls and control enhancements are not allocated to baselines in this table. See **Appendix F** for control selection and implementation guidance.					

Commented [A1]: Please note that this column, "Privacy-Related" is new to Rev. 5. All content in this column is also new.

In Rev.4, there was a column titled, "Priority" that was removed.