



TALATEK LLC
COMPLIANCE THROUGH RISK MANAGEMENT

NIST SP 800-53 Rev. 4

Recommended Security Controls for Federal Information Systems and Organizations

Final – May 2013

CONTROL FAMILY	
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
PC	Privacy Controls

LEGEND: C - Confidentiality I - Integrity A - Availability

ACCESS CONTROL (AC)

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
AC-1	Access Control Policy and Procedures	P1	C I A	AC-1	AC-1	AC-1	PM-9
AC-2	Account Management	P1	C	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (12) (13)	AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13
AC-3	Access Enforcement	P1	C	AC-3	AC-3	AC-3	AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3
AC-4	Information Flow Enforcement	P1	C	Not Selected	AC-4	AC-4	AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18
AC-5	Separation of Duties	P1	C	Not Selected	AC-5	AC-5	AC-3, AC-6, PE-3, PE-4, PS-2
AC-6	Least Privilege	P1	C	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)	AC-2, AC-3, AC-5, CM-6, CM-7, PL-2
AC-7	Unsuccessful Logon Attempts	P2	C	AC-7	AC-7	AC-7	AC-2, AC-9, AC-14, IA-5
AC-8	System Use Notification	P1	C	AC-8	AC-8	AC-8	None
AC-9	Previous Logon (Access) Notification	P0	C	Not Selected	Not Selected	Not Selected	AC-7, PL-4
AC-10	Concurrent Session Control	P2	C	Not Selected	Not Selected	AC-10	None
AC-11	Session Lock	P3	C	Not Selected	AC-11 (1)	AC-11 (1)	AC-7
AC-12	Session Termination	P2	C I A	Not Selected	AC-12	AC-12	SC-10, SC-23
AC-13	Supervision and Review (Withdrawn) Incorporated into AC-2 and AU-6			---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P1	C I	AC-14	AC-14	AC-14	CP-2, IA-2
AC-15	Automated Marking (Withdrawn) Incorporated into MP-3			---	---	---	---
AC-16	Security Attributes	P0	C	Not Selected	Not Selected	Not Selected	AC-3, AC-4, AC-6, AC-21, AU-2, AU-10, MP-3, SC-16
AC-17	Remote Access	P1	C	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)	AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
AC-18	Wireless Access	P1	C	AC-18	AC-18 (1)	AC-18 (1) (4) (5)	AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4
AC-19	Access Control for Mobile Devices	P1	C	AC-19	AC-19 (5)	AC-19 (5)	AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4
AC-20	Use of External Information Systems	P1	C	AC-20	AC-20 (1) (2)	AC-20 (1) (2)	AC-3, AC-17, AC-19, CA-3, PL-4, SA-9
AC-21	Information Sharing	P2	C	Not Selected	AC-21	AC-21	AC-3
AC-22	Publicly Accessible Content	P2	C I	AC-22	AC-22	AC-22	AC-3, AC-4, AT-2, AT-3, AU-13
AC-23	Data Mining Protection	P0	C I	Not Selected	Not Selected	Not Selected	None
AC-24	Access Control Decisions	P0	C I	Not Selected	Not Selected	Not Selected	None
AC-25	Reference Monitor	P0	C I A	Not Selected	Not Selected	Not Selected	AC-3, AC-16, SC-3, SC-39

AWARENESS AND TRAINING (AT)

AT-1	Security Awareness and Training Policy and Procedures	P1	C I A	AT-1	AT-1	AT-1	PM-9
AT-2	Security Awareness Training	P1	C I A	AT-2	AT-2 (2)	AT-2 (2)	AT-3, AT-4, PL-4
AT-3	Role-Based Security Training	P1	C I A	AT-3	AT-3	AT-3	AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16
AT-4	Security Training Records	P3	C I A	AT-4	AT-4	AT-4	AT-2, AT-3, PM-14
AT-5	Contacts with Security Groups and Associations (Withdrawn) Incorporated into PM-15			---	---	---	---

AUDIT AND ACCOUNTABILITY (AU)

AU-1	Audit and Accountability Policy and Procedures	P1	C I A	AU-1	AU-1	AU-1	PM-9
AU-2	Audit Events	P1	C I A	AU-2	AU-2 (3)	AU-2 (3)	AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, SI-4
AU-3	Content of Audit Records	P1	C I A	AU-3	AU-3 (1)	AU-3 (1) (2)	AU-2, AU-8, AU-12, SI-11
AU-4	Audit Storage Capacity	P1	I A	AU-4	AU-4	AU-4	AU-2, AU-5, AU-6, AU-7, AU-11, SI-4
AU-5	Response to Audit Processing Failures	P1	I A	AU-5	AU-5	AU-5 (1) (2)	AU-4, SI-12

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
AU-6	Audit Review, Analysis, and Reporting	P1	C I A	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)	AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7
AU-7	Audit Reduction and Report Generation	P2	I A	Not Selected	AU-7 (1)	AU-7 (1)	AU-6
AU-8	Time Stamps	P1	I	AU-8	AU-8 (1)	AU-8 (1)	AU-3, AU-12
AU-9	Protection of Audit Information	P1	C I	AU-9	AU-9 (4)	AU-9 (2) (3) (4)	AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6
AU-10	Non-repudiation	P1	I	Not Selected	Not Selected	AU-10	SC-8, SC-12, SC-13, SC-16, SC-17, SC-23
AU-11	Audit Record Retention	P3	A	AU-11	AU-11	AU-11	AU-4, AU-5, AU-9, MP-6
AU-12	Audit Generation	P1	C I A	AU-12	AU-12	AU-12 (1) (3)	AC-3, AU-2, AU-3, AU-6, AU-7
AU-13	Monitoring for Information Disclosure	P0	C I	Not Selected	Not Selected	Not Selected	PE-3, SC-7
AU-14	Session Audit	P0	C	Not Selected	Not Selected	Not Selected	AC-3, AU-4, AU-5, AU-9, AU-11
AU-15	Alternate Audit Capability	P0	I A	Not Selected	Not Selected	Not Selected	AU-5
AU-16	Cross-Organizational Auditing	P0	C I A	Not Selected	Not Selected	Not Selected	AU-6

SECURITY ASSESSMENT AND AUTHORIZATION (CA)

CA-1	Security Assessment and Authorization Policies and Procedures	P1	C I A	CA-1	CA-1	CA-1	PM-9
CA-2	Security Assessments	P2	C I A	CA-2	CA-2 (1)	CA-2 (1) (2)	CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4
CA-3	System Interconnections	P1	I	CA-3	CA-3 (5)	CA-3 (5)	AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4
CA-4	Security Certification (Withdrawn) Incorporated into CA-2			---	---	---	---
CA-5	Plan of Action and Milestones	P3	C I A	CA-5	CA-5	CA-5	CA-2, CA-7, CM-4, PM-4
CA-6	Security Authorization	P3	C I A	CA-6	CA-6	CA-6	CA-2, CA-7, PM-9, PM-10
CA-7	Continuous Monitoring	P3	C I A	CA-7	CA-7 (1)	CA-7 (1)	CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
CA-8	Penetration Testing	P1	I A	Not Selected	Not Selected	CA-8	SA-12
CA-9	Internal System Connections	P2	C I A	CA-9	CA-9	CA-9	AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4

CONFIGURATION MANAGEMENT (CM)

CM-1	Configuration Management Policy and Procedures	P1	C I A	CM-1	CM-1	CM-1	PM-9
CM-2	Baseline Configuration	P1	I A	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)	CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7
CM-3	Configuration Change Control	P1	C I A	Not Selected	CM-3 (2)	CM-3 (1) (2)	CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12
CM-4	Security Impact Analysis	P2	C I A	CM-4	CM-4	CM-4 (1)	CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2
CM-5	Access Restrictions for Change	P1	C I A	Not Selected	CM-5	CM-5 (1) (2) (3)	AC-3, AC-6, PE-3
CM-6	Configuration Settings	P1	C I	CM-6	CM-6	CM-6 (1) (2)	AC-19, CM-2, CM-3, CM-7, SI-4
CM-7	Least Functionality	P1	C I A	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)	AC-6, CM-2, RA-5, SA-5, SC-7
CM-8	Information System Component Inventory	P1	C I A	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)	CM-2, CM-6, PM-5
CM-9	Configuration Management Plan	P1	C I A	Not Selected	CM-9	CM-9	CM-2, CM-3, CM-4, CM-5, CM-8, SA-10
CM-10	Software Usage Restrictions	P2	C I A	CM-10	CM-10	CM-10	AC-17, CM-8, SC-7
CM-11	User-Installed Software	P1	C I A	CM-11	CM-11	CM-11	AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4

CONTINGENCY PLANNING (CP)

CP-1	Contingency Planning Policy and Procedures	P1	C I A	CP-1	CP-1	CP-1	PM-9
CP-2	Contingency Plan	P1	A	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)	AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11
CP-3	Contingency Training	P2	A	CP-3	CP-3	CP-3 (1)	AT-2, AT-3, CP-2, IR-2
CP-4	Contingency Plan Testing	P2	A	CP-4	CP-4 (1)	CP-4 (1) (2)	CP-2, CP-3, IR-3
CP-5	Contingency Plan Update (Withdrawn) Incorporated into CP-2			---	---	---	---

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
CP-6	Alternate Storage Site	P1	A	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)	CP-2, CP-7, CP-9, CP-10, MP-4
CP-7	Alternate Processing Site	P1	A	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)	CP-2, CP-6, CP-8, CP-9, CP-10, MA-6
CP-8	Telecommunications Services	P1	A	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)	CP-2, CP-6, CP-7
CP-9	Information System Backup	P1	A	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)	CP-2, CP-6, MP-4, MP-5, SC-13
CP-10	Information System Recovery and Reconstitution	P1	A	CP-10	CP-10 (2)	CP-10 (2) (4)	CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24
CP-11	Predictable Failure Prevention	P0	C I A	Not Selected	Not Selected	Not Selected	None
CP-12	Alternate Communications Protocols	P0	A	Not Selected	Not Selected	Not Selected	None
CP-13	Safe Mode	P0	C I A	Not Selected	Not Selected	Not Selected	CP-2

IDENTIFICATION AND AUTHENTICATION (IA)

IA-1	Identification and Authentication Policy and Procedures	P1	C I A	IA-1	IA-1	IA-1	PM-9
IA-2	Identification and Authentication (Organizational Users)	P1	C	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)	AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8
IA-3	Device Identification and Authentication	P1	C	Not Selected	IA-3	IA-3	AC-17, AC-18, AC-19, CA-3, IA-4, IA-5
IA-4	Identifier Management	P1	C	IA-4	IA-4	IA-4	AC-2, IA-2, IA-3, IA-5, IA-8, SC-37
IA-5	Authenticator Management	P1	C	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)	AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28
IA-6	Authenticator Feedback	P1	C	IA-6	IA-6	IA-6	PE-18
IA-7	Cryptographic Module Authentication	P1	C	IA-7	IA-7	IA-7	SC-12, SC-13
IA-8	Identification and Authentication (Non-Organizational Users)	P1	C	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8
IA-9	Service Identification and Authentication	P0	C	Not Selected	Not Selected	Not Selected	None
IA-10	Adaptive Identification and Authentication	P0	C I A	Not Selected	Not Selected	Not Selected	AU-6, SI-4
IA-11	Re-authentication	P0	C I A	Not Selected	Not Selected	Not Selected	AC-11

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
IR-1	Incident Response Policy and Procedures	P1	C I A	IR-1	IR-1	IR-1	PM-9
IR-2	Incident Response Training	P2	C I A	IR-2	IR-2	IR-2 (1) (2)	AT-3, CP-3, IR-8
IR-3	Incident Response Testing	P2	C I A	Not Selected	IR-3 (2)	IR-3 (2)	CP-4, IR-8
IR-4	Incident Handling	P1	C I A	IR-4	IR-4 (1)	IR-4 (1) (4)	AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7
IR-5	Incident Monitoring	P1	C I A	IR-5	IR-5	IR-5 (1)	AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7
IR-6	Incident Reporting	P1	C I A	IR-6	IR-6 (1)	IR-6 (1)	IR-4, IR-5, IR-8
IR-7	Incident Response Assistance	P3	C I A	IR-7	IR-7 (1)	IR-7 (1)	AT-2, IR-4, IR-6, IR-8, SA-9
IR-8	Incident Response Plan	P1	C I A	IR-8	IR-8	IR-8	MP-2, MP-4, MP-5
IR-9	Information Spillage Response	P0	C I	Not Selected	Not Selected	Not Selected	None
IR-10	Integrated Information Security Analysis Team	P0	C I A	Not Selected	Not Selected	Not Selected	None

MAINTENANCE (MA)

MA-1	System Maintenance Policy and Procedures	P1	C I A	MA-1	MA-1	MA-1	PM-9
MA-2	Controlled Maintenance	P2	A	MA-2	MA-2	MA-2 (2)	CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2
MA-3	Maintenance Tools	P2	I A	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)	MA-2, MA-5, MP-6
MA-4	Nonlocal Maintenance	P1	C I A	MA-4	MA-4 (2)	MA-4 (2) (3)	AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17
MA-5	Maintenance Personnel	P1	C	MA-5	MA-5	MA-5 (1)	AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3
MA-6	Timely Maintenance	P2	I	Not Selected	MA-6	MA-6	CM-8, CP-2, CP-7, SA-14, SA-15

MEDIA PROTECTION (MP)

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
MP-1	Media Protection Policy and Procedures	P1	C I A	MP-1	MP-1	MP-1	PM-9
MP-2	Media Access	P1	C	MP-2	MP-2	MP-2	AC-3, IA-2, MP-4, PE-2, PE-3, PL-2
MP-3	Media Marking	P2	C	Not Selected	MP-3	MP-3	AC-16, PL-2, RA-3
MP-4	Media Storage	P1	C	Not Selected	MP-4	MP-4	CP-6, CP-9, MP-2, MP-7, PE-3
MP-5	Media Transport	P1	C	Not Selected	MP-5 (4)	MP-5 (4)	AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28
MP-6	Media Sanitization	P1	C	MP-6	MP-6	MP-6 (1) (2) (3)	MA-2, MA-4, RA-3, SC-4
MP-7	Media Use	P1	C	MP-7	MP-7 (1)	MP-7 (1)	AC-19, PL-4
MP-8	Media Downgrading	P0	C	Not Selected	Not Selected	Not Selected	None

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

PE-1	Physical and Environmental Protection Policy and Procedures	P1	C I A	PE-1	PE-1	PE-1	PM-9
PE-2	Physical Access Authorizations	P1	C	PE-2	PE-2	PE-2	PE-3, PE-4, PS-3
PE-3	Physical Access Control	P1	C	PE-3	PE-3	PE-3 (1)	AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3
PE-4	Access Control for Transmission Medium	P1	C	Not Selected	PE-4	PE-4	MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8
PE-5	Access Control for Output Devices	P2	C	Not Selected	PE-5	PE-5	PE-2, PE-3, PE-4, PE-18
PE-6	Monitoring Physical Access	P1	C I A	PE-6	PE-6 (1)	PE-6 (1) (4)	CA-7, IR-4, IR-8
PE-7	Visitor Control (Withdrawn) Incorporated into PE-2 and PE-3			---	---	---	---
PE-8	Visitor Access Records	P3	C	PE-8	PE-8	PE-8 (1)	None
PE-9	Power Equipment and Cabling	P1	I	Not Selected	PE-9	PE-9	PE-4
PE-10	Emergency Shutoff	P1	I	Not Selected	PE-10	PE-10	PE-15
PE-11	Emergency Power	P1	I A	Not Selected	PE-11	PE-11 (1)	AT-3, CP-2, CP-7
PE-12	Emergency Lighting	P1	A	PE-12	PE-12	PE-12	CP-2, CP-7

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
PE-13	Fire Protection	P1	A	PE-13	PE-13 (3)	PE-13 (1) (2) (3)	None
PE-14	Temperature and Humidity Controls	P1	A	PE-14	PE-14	PE-14	AT-3
PE-15	Water Damage Protection	P1	A	PE-15	PE-15	PE-15 (1)	AT-3
PE-16	Delivery and Removal	P2	C	PE-16	PE-16	PE-16	CM-3, MA-2, MA-3, MP-5, SA-12
PE-17	Alternate Work Site	P2	A	Not Selected	PE-17	PE-17	AC-17, CP-7
PE-18	Location of Information System Components	P3	C I A	Not Selected	Not Selected	PE-18	CP-2, PE-19, RA-3
PE-19	Information Leakage	P0	C	Not Selected	Not Selected	Not Selected	None
PE-20	Asset Monitoring and Tracking	P0	C I A	Not Selected	Not Selected	Not Selected	CM-8

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
PL-1	Security Planning Policy and Procedures	P1	C I A	PL-1	PL-1	PL-1	PM-9
PL-2	System Security Plan	P1	C I A	PL-2	PL-2 (3)	PL-2 (3)	AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17
PL-3	System Security Plan Update			---	---	---	---
PL-4	Rules of Behavior	P2	C I A	PL-4	PL-4 (1)	PL-4 (1)	AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5
PL-5	Privacy Impact Assessment (Withdrawn) Incorporated into Appendix J, AR-2			---	---	---	---
PL-6	Security-Related Activity Planning (Withdrawn) Incorporated into PL-2			---	---	---	---
PL-7	Security Concept of Operations	P0	C I A	Not Selected	Not Selected	Not Selected	PL-2
PL-8	Information Security Architecture	P1	C I A	Not Selected	PL-8	PL-8	CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, Appendix J
PL-9	Central Management	P0	C I A	Not Selected	Not Selected	Not Selected	AC-2 (1) (2) (3) (4); AC-17 (1) (2) (3) (9); AC-18 (1) (3) (4) (5); AC-19 (4) (6) (8) (9); AC-22; AC-23; AT-2 (1) (2); AT-3 (1) (2) (3); AT-4; AT-5; AU-6 (1) (3) (5) (6) (9); AU-7 (1) (2); AU-11, AU-13, AU-16, CA-2 (1) (2) (3); CA-3 (1) (2) (3); CA-7 (1); CA-9; CM-2 (1) (2); CM-3 (1) (4); CM-4; CM-6 (1); CM-7 (4) (5); CM-8 (all); CM-9 (1); CM-10; CM-11; CP-7 (all); CP-8 (all); SC-43; SI-2; SI-3; SI-7; SI-8

Control ID	Control Name	Related Controls
PM-1	Information Security Program	PM-8
PM-2	Senior Information Security Officer	None
PM-3	Information Security Resources	PM-4, SA-2
PM-4	Plan of Action and Milestone Process	CA-5
PM-5	Information System Inventory	None
PM-6	Information Security Measures of Performance	None
PM-7	Enterprise Architecture	PL-2, PL-8, PM-11, RA-2, SA-3
PM-8	Critical Infrastructure Plan	PM-1, PM-9, PM-11, RA-3
PM-9	Risk Management Strategy	RA-3
PM-10	Security Authorization Process	CA-6
PM-11	Mission/Business Process Definition	PM-7, PM-8, RA-2
PM-12	Insider Threat Program	AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-1, PM-14, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4
PM-13	Information Security Workforce	AT-2, AT-3
PM-14	Testing, Training, and Monitoring	AT-3, CA-7, CP-4, IR-3, SI-4
PM-15	Contacts with Security Groups and Associations	SI-5
PM-16	Threat Awareness Program	PM-12

PERSONNEL SECURITY (PS)

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
PS-1	Personnel Security Policy and Procedures	P1	C I A	PS-1	PS-1	PS-1	PM-9
PS-2	Position Risk Designation	P1	C I A	PS-2	PS-2	PS-2	AT-3, PL-2, PS-3
PS-3	Personnel Screening	P1	C	PS-3	PS-3	PS-3	AC-2, IA-4, PE-2, PS-2
PS-4	Personnel Termination	P1	C A	PS-4	PS-4	PS-4 (2)	AC-2, IA-4, PE-2, PS-5, PS-6
PS-5	Personnel Transfer	P2	C	PS-5	PS-5	PS-5	AC-2, IA-4, PE-2, PS-4
PS-6	Access Agreements	P3	C	PS-6	PS-6	PS-6	PL-4, PS-2, PS-3, PS-8
PS-7	Third-Party Personnel Security	P1	C I A	PS-7	PS-7	PS-7	PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21
PS-8	Personnel Sanctions	P3	C I A	PS-8	PS-8	PS-8	PL-4, PS-6

RISK ASSESSMENT (RA)

RA-1	Risk Assessment Policy and Procedures	P1	C I A	RA-1	RA-1	RA-1	PM-9
RA-2	Security Categorization	P1	C I A	RA-2	RA-2	RA-2	CM-8, MP-4, RA-3, SC-7
RA-3	Risk Assessment	P1	C I A	RA-3	RA-3	RA-3	RA-2, PM-9
RA-4	Risk Assessment Update (Withdrawn) Incorporated into RA-3			---	---	---	---
RA-5	Vulnerability Scanning	P1	C I A	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)	CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2
RA-6	Technical Surveillance Countermeasures Survey	P0	C I A	Not Selected	Not Selected	Not Selected	None

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
SA-1	System and Services Acquisition Policy and Procedures	P1	C I A	SA-1	SA-1	SA-1	PM-9
SA-2	Allocation of Resources	P1	C I A	SA-2	SA-2	SA-2	PM-3, PM-11
SA-3	System Development Life Cycle	P1	C I A	SA-3	SA-3	SA-3	AT-3, PM-7, SA-8
SA-4	Acquisition Process	P1	C I A	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (9) (10)	CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12
SA-5	Information System Documentation	P2	C I A	SA-5	SA-5	SA-5	CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4
SA-6	Software Usage Restrictions (Withdrawn) Incorporated into CM-10 and SI-7			---	---	---	---
SA-7	User Installed Software (Withdrawn) Incorporated into CM-11 and SI-7			---	---	---	---
SA-8	Security Engineering Principles	P1	I A	Not Selected	SA-8	SA-8	PM-7, SA-3, SA-4, SA-17, SC-2, SC-3
SA-9	External Information System Services	P1	C I A	SA-9	SA-9 (2)	SA-9 (2)	CA-3, IR-7, PS-7
SA-10	Developer Configuration Management	P1	C I A	Not Selected	SA-10	SA-10	CM-3, CM-4, CM-9, SA-12, SI-2
SA-11	Developer Security Testing and Evaluation	P1	C I A	Not Selected	SA-11	SA-11	CA-2, CM-4, SA-3, SA-4, SA-5, SI-2
SA-12	Supply Chain Protection	P1	C I A	Not Selected	Not Selected	SA-12	AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7
SA-13	Trustworthiness	P0	C I A	Not Selected	Not Selected	Not Selected	RA-2, SA-4, SA-8, SA-14, SC-3
SA-14	Criticality Analysis	P0	C I A	Not Selected	Not Selected	Not Selected	CP-2, PL-2, PL-8, PM-1, SA-8, SA-12, SA-13, SA-15, SA-20
SA-15	Development Process, Standards, and Tools	P2	C I A	Not Selected	Not Selected	SA-15	SA-3, SA-8
SA-16	Developer-Provided Training	P2	C I A	Not Selected	Not Selected	SA-16	AT-2, AT-3, SA-5
SA-17	Developer Security Architecture and Design	P1	C I A	Not Selected	Not Selected	SA-17	PL-8, PM-7, SA-3, SA-8

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
SA-18	Tamper Resistance and Detection	P0	C I A	Not Selected	Not Selected	Not Selected	PE-3, SA-12, SI-7
SA-19	Component Authenticity	P0	C I A	Not Selected	Not Selected	Not Selected	PE-3, SA-12, SI-7
SA-20	Customized Development of Critical Components	P0	C I A	Not Selected	Not Selected	Not Selected	CP-2, SA-8, SA-14
SA-21	Developer Screening	P0	C I A	Not Selected	Not Selected	Not Selected	PS-3, PS-7
SA-22	Unsupported System Components	P0	C I A	Not Selected	Not Selected	Not Selected	PL-2, SA-3

SYSTEM AND COMMUNICATIONS PROTECTION (SC)

SC-1	System and Communications Protection Policy and Procedures	P1	C I A	SC-1	SC-1	SC-1	PM-9
SC-2	Application Partitioning	P1	C I	Not Selected	SC-2	SC-2	SA-4, SA-8, SC-3
SC-3	Security Function Isolation	P1	I	Not Selected	Not Selected	SC-3	AC-3, AC-6, SA-4, SA-5, SA-8, SA-13, SC-2, SC-7, SC-39
SC-4	Information in Shared Resources	P1	C I	Not Selected	SC-4	SC-4	AC-3, AC-4, MP-6
SC-5	Denial of Service Protection	P1	A	SC-5	SC-5	SC-5	SC-6, SC-7
SC-6	Resource Availability	P0	A	Not Selected	Not Selected	Not Selected	None
SC-7	Boundary Protection	P1	C	SC-7	SC-7 (3) (4) (5) (7)	36) SC-7 (3) (4) (5) (7) (8) (18) (21)	AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13
SC-8	Transmission Confidentiality and Integrity	P1	C I	Not Selected	SC-8 (1)	SC-8 (1)	AC-17, PE-4
SC-9	Transmission Confidentiality (Withdrawn) Incorporated into SC-8			---	---	---	---
SC-10	Network Disconnect	P2	C I A	Not Selected	SC-10	SC-10	None
SC-11	Trusted Path	P0	C I	Not Selected	Not Selected	Not Selected	AC-16, AC-25
SC-12	Cryptographic Key Establishment and Management	P1	I A	SC-12	SC-12	SC-12 (1)	SC-13, SC-17

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
SC-13	Cryptographic Protection	P1	C I	SC-13	SC-13	SC-13	AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7
SC-14	Public Access Protections (Withdrawn) Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10			---	---	---	---
SC-15	Collaborative Computing Devices	P1	C	SC-15	SC-15	SC-15	AC-21
SC-16	Transmission of Security Attributes	P0	C	Not Selected	Not Selected	Not Selected	AC-3, AC-4, AC-16
SC-17	Public Key Infrastructure Certificates	P1	C I	Not Selected	SC-17	SC-17	SC-12
SC-18	Mobile Code	P2	C I A	Not Selected	SC-18	SC-18	AU-2, AU-12, CM-2, CM-6, SI-3
SC-19	Voice Over Internet Protocol	P1	C I A	Not Selected	SC-19	SC-19	CM-6, SC-7, SC-15
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	C I A	SC-20	SC-20	SC-20	AU-10, SC-8, SC-12, SC-13, SC-21, SC-22
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	C I A	SC-21	SC-21	SC-21	SC-20, SC-22
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	C I A	SC-22	SC-22	SC-22	SC-2, SC-20, SC-21, SC-24
SC-23	Session Authenticity	P1	C I A	Not Selected	SC-23	SC-23	SC-8, SC-10, SC-11
SC-24	Fail in Known State	P1	C I A	Not Selected	Not Selected	SC-24	CP-2, CP-10, CP-12, SC-7, SC-22
SC-25	Thin Nodes	P0	C I A	Not Selected	Not Selected	Not Selected	SC-30
SC-26	Honeypots	P0	C I A	Not Selected	Not Selected	Not Selected	SC-30, SC-44, SI-3, SI-4
SC-27	Platform-Independent Applications	P0	A	Not Selected	Not Selected	Not Selected	SC-29
SC-28	Protection of Information at Rest	P1	C I	Not Selected	SC-28	SC-28	AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
SC-29	Heterogeneity	P0	C I A	Not Selected	Not Selected	Not Selected	SA-12, SA-14, SC-27
SC-30	Concealment and Misdirection	P0	C I A	Not Selected	Not Selected	Not Selected	SC-26, SC-29, SI-14
SC-31	Covert Channel Analysis	P0	C	Not Selected	Not Selected	Not Selected	AC-3, AC-4, PL-2
SC-32	Information System Partitioning	P0	C I A	Not Selected	Not Selected	Not Selected	AC-4, SA-8, SC-2, SC-3, SC-7
SC-33	Transmission Preparation Integrity (Withdrawn) Incorporated into SC-8			---	---	---	---
SC-34	Non-Modifiable Executable Programs	P0	I	Not Selected	Not Selected	Not Selected	AC-3, SI-7
SC-35	Honeyclients	P0	C I A	Not Selected	Not Selected	Not Selected	SC-26, SC-44, SI-3, SI-4
SC-36	Distributed Processing and Storage	P0	A	Not Selected	Not Selected	Not Selected	CP-6, CP-7
SC-37	Out-of-Band Channels	P0	C I A	Not Selected	Not Selected	Not Selected	AC-2, CM-3, CM-5, CM-7, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7
SC-38	Operations Security	P0	C	Not Selected	Not Selected	Not Selected	RA-2, RA-5, SA-12
SC-39	Process Isolation	P1	C I A	SC-39	SC-39	SC-39	AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3
SC-40	Wireless Link Protection	P0	C I A	Not Selected	Not Selected	Not Selected	AC-18, SC-5
SC-41	Port and I/O Device Access	P0	C I A	Not Selected	Not Selected	Not Selected	None
SC-42	Sensor Capability and Data	P0	C I A	Not Selected	Not Selected	Not Selected	None
SC-43	Usage Restrictions	P0	C I	Not Selected	Not Selected	Not Selected	CM-6, SC-7
SC-44	Detonation Chambers	P0	C A	Not Selected	Not Selected	Not Selected	SC-7, SC-25, SC-26, SC-30

Control ID	Control Name	Priority	C I A	Control Baseline Low	Control Baseline Moderate	Control Baseline High	Related Controls
SI-1	System and Information Integrity Policy and Procedures	P1	C I A	SI-1	SI-1	SI-1	PM-9
SI-2	Flaw Remediation	P1	I	SI-2	SI-2 (2)	SI-2 (1) (2)	CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11
SI-3	Malicious Code Protection	P1	C I A	SI-3	SI-3 (1) (2)	SI-3 (1) (2)	CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7
SI-4	Information System Monitoring	P1	C I A	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)	AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7
SI-5	Security Alerts, Advisories, and Directives	P1	C I A	SI-5	SI-5	SI-5 (1)	SI-2
SI-6	Security Function Verification	P1	I A	Not Selected	Not Selected	SI-6	CA-7, CM-6
SI-7	Software, Firmware, and Information Integrity	P1	I	Not Selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)	SA-12, SC-8, SC-13, SI-3
SI-8	Spam Protection	P2	C I A	Not Selected	SI-8 (1) (2)	SI-8 (1) (2)	AT-2, AT-3, SC-5, SC-7, SI-3
SI-9	Information Input Restrictions (Withdrawn) Incorporated into AC-2, AC-3, AC-5, AC-6			---	---	---	---
SI-10	Information Input Validation	P1	I	Not Selected	SI-10	SI-10	None
SI-11	Error Handling	P2	C I A	Not Selected	SI-11	SI-11	AU-2, AU-3, SC-31
SI-12	Information Handling and Retention	P2	C	SI-12	SI-12	SI-12	AC-16, AU-5, AU-11, MP-2, MP-4
SI-13	Predictable Failure Prevention	P0	A	Not Selected	Not Selected	Not Selected	CP-2, CP-10, MA-6
SI-14	Non-Persistence	P0	C I A	Not Selected	Not Selected	Not Selected	SC-30, SC-34
SI-15	Information Output Filtering	P0	I	Not Selected	Not Selected	Not Selected	SI-3, SI-4
SI-16	Memory Protection	P1	C I A	Not Selected	SI-16	SI-16	AC-25, SC-3
SI-17	Fail-Safe Procedures	P0	I A	Not Selected	Not Selected	Not Selected	CP-12, CP-13, SC-24, SI-13

Control ID	Family	Related Controls
AP	Authority and Purpose	
AP-1	Authority to Collect	AR-2, DM-1, TR-1, TR-2
AP-2	Purpose Specification	AR-2, AR-4, AR-5, DM-1, DM-2, TR-1, TR-2, UL-1, UL-2
AR	Accountability, Audit, and Risk Management	
AR-1	Governance and Privacy Program	None
AR-2	Privacy Impact and Risk Assessment	None
AR-3	Privacy Requirements for Contractors and Service Providers	AR-1, AR-5, SA-4
AR-4	Privacy Monitoring and Auditing	AR-6, AR-7, AU-1, AU-2, AU-3, AU-6, AU-12, CA-7, TR-1, UL-2
AR-5	Privacy Awareness and Training	AR-3, AT-2, AT-3, TR-1
AR-6	Privacy Reporting	None
AR-7	Privacy-Enhanced System Design and Development	AC-6, AR-4, AR-5, DM-2, TR-1
AR-8	Accounting of Disclosures	IP-2
DI	Data Quality and Integrity	
DI-1	Data Quality	AP-2, DI-2, DM-1, IP-3, SI-10
DI-2	Data Integrity and Data Integrity Board	AC-1, AC-3, AC-4, AC-6, AC-17, AC-22, AU-2, AU-3, AU-6, AU-10, AU-11, DI-1, SC-8, SC-28, UL-2
DM	Data Minimization and Retention	
DM-1	Minimization of Personally Identifiable Information	AP-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1
DM-2	Data Retention and Disposal	AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1
DM-3	Minimization of PII Used in Testing, Training and Research	None
IP	Individual Participation and Redress	
IP-1	Consent	AC-2, AP-1, TR-1, TR-2
IP-2	Individual Access	AR-8, IP-3, TR-1, TR-2
IP-3	Redress	IP-2, TR-1, TR-2, UL-2
IP-4	Complaint Management	AR-6, IP-3

Control ID	Family	Related Controls
SE	Security	
SE-1	Inventory of Personally Identifiable Information	AR-1, AR-4, AR-5, AT-1, DM-1, PM-5, UL-3
SE-2	Privacy Incident Response	AR-1, AR-4, AR-5, AR-6, AU-1 through AU-14, IR-1 through IR-8, RA-1
TR	Transparency	
TR-1	Privacy Notice	AP-1, AP-2, AR-1, AR-2, IP-1, IP-2, IP-3, UL-1, UL-2
TR-2	System of Records Notices and Privacy Act Statements	DI-2
TR-3	Dissemination of Privacy Program Information	AR-6
UL	Use Limitation	
UL-1	Internal Use	AP-2, AR-2, AR-3, AR-4, AR-5, IP-1, TR-1, TR-2
UL-2	Information Sharing with Third Parties	AR-3, AR-4, AR-5, AR-8, AP-2, DI-1, DI-2, IP-1, TR-1

PRIORITY CODE

Priority Code 1 (P1)	FIRST	Implement P1 security controls first.
Priority Code 2 (P2)	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 (P3)	LAST	Implement P3 security controls after implementation of P2 and P3 controls.
Unspecified Priority Code (P0)	NONE	Security control not selected for any baseline.



COMPLIANCE THROUGH RISK MANAGEMENT