TALATEK LLC
COMPLIANCE THROUGH RISK MANAGEMENT

NIST 800-53 Rev 5.0

Security and Privacy Controls for Information Systems and Organizations

January 2021

CONTROL FAMILY

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
AC-1	Policy and Procedures				O	x	x	x	x
AC-2	Account Management		x		O		x	x	x
AC-2(1)	Automated System Account Management				O			x	x
AC-2(2)	Automated Temporary and Emergency Account Management				S			x	x
AC-2(3)	Disable Accounts				S			x	x
AC-2(4)	Automated Audit Actions				S			x	x
AC-2(5)	Inactivity Logout				O/S			x	x
AC-2(6)	Dynamic Privilege Management				S				
AC-2(7)	Privileged User Accounts				O				
AC-2(8)	Dynamic Account Management				S				
AC-2(9)	Restrictions on Use of Shared and Group Accounts				O				
AC-2(10)	Shared and Group Account Credential Change			→ AC-2k					
AC-2(11)	Usage Conditions				S				x
AC-2(12)	Account Monitoring for Atypical Usage				O/S				x
AC-2(13)	Disable Accounts for High-Risk Individuals				O			x	x
AC-3	Access Enforcement				S		x	x	x
AC-3(2)	Dual Authorization				S				
AC-3(3)	Mandatory Access Control				S				
AC-3(4)	Discretionary Access Control				S				
AC-3(5)	Security-Relevant Information				S				
AC-3(7)	Role-Based Access Control				O/S				
AC-3(8)	Revocation of Access Authorizations				O/S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
AC-3(9)	Controlled Release				O/S				
AC-3(10)	Audited Override of Access Control Mechanisms				O				
AC-3(11)	Restrict Access to Specific Information Types	x			S				
AC-3(12)	Assert and Enforce Application Access	x			S				
AC-3(13)	Attribute-Based Access Control	x			S				
AC-3(14)	Individual Access	x			S	x			
AC-3(15)	Discretionary and Mandatory Access Control	x			S				
AC-4	Information Flow Enforcement				S			x	x
AC-4(1)	Object Security and Privacy Attributes				S				
AC-4(2)	Processing Domains				S				
AC-4(3)	Dynamic Information Flow Control				S				
AC-4(4)	Flow Control of Encrypted Information				S				x
AC-4(5)	Embedded Data Types				S				
AC-4(6)	Metadata				S				
AC-4(7)	One-Way Flow Mechanisms				S				
AC-4(8)	Security and Privacy Policy Filters				S				
AC-4(9)	Human Reviews				O/S				
AC-4(10)	Enable and Disable Security or Privacy Policy Filters				S				
AC-4(11)	Configuration of Security or Privacy Policy Filters				S				
AC-4(12)	Data Type Identifiers				S				
AC-4(13)	Decomposition Into Policy-Relevant Subcomponents				S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
AC-4(14)	Security or Privacy Policy Filter Constraints				S				
AC-4(15)	Detection of Unsanctioned Information				S				
AC-4(17)	Domain Authentication				S				
AC-4(18)	Security Attribute Binding			→ AC-16					
AC-4(19)	Validation of Metadata				S				
AC-4(20)	Approved Solutions				O				
AC-4(21)	Physical or Logical Separation of Information Flows				O/S				
AC-4(22)	Access Only				S				
AC-4(23)	Modify Non-Releasable Information	x			O/S				
AC-4(24)	Internal Normalized Format	x			S				
AC-4(25)	Data Sanitization	x			S				
AC-4(26)	Audit Filtering Actions	x			O/S				
AC-4(27)	Redundant/Independent Filtering Mechanisms	x			S				
AC-4(28)	Linear Filter Pipelines	x			S				
AC-4(29)	Filter Orchestration Engines	x			O/S				
AC-4(30)	Filter Mechanisms Using Multiple Processes	x			S				
AC-4(31)	Failed Content Transfer Prevention	x			S				
AC-4(32)	Process Requirements for Information Transfer	x			S				
AC-5	Separation of Duties				O			x	x
AC-6	Least Privilege				O			x	x
AC-6(1)	Authorize Access to Security Functions				O			x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
AC-6(2)	Non-Privileged Access for Nonsecurity Functions				O			x	x
AC-6(3)	Network Access to Privileged Commands				O				x
AC-6(4)	Separate Processing Domains				O/S				
AC-6(5)	Privileged Accounts				O			x	x
AC-6(6)	Privileged Access by Non-Organizational Users				O				
AC-6(7)	Review of User Privileges				O			x	x
AC-6(8)	Privilege Levels for Code Execution				S				
AC-6(9)	Log Use of Privileged Functions				S			x	x
AC-6(10)	Prohibit Non-Privileged Users from Executing Privileged Functions				S			x	x
AC-7	Unsuccessful Logon Attempts				S		x	x	x
AC-7(2)	Purge or Wipe Mobile Device				S				
AC-7(3)	Biometric Attempt Limiting	x			O				
AC-7(4)	Use of Alternate Authentication Factor	x			O/S				
AC-8	System Use Notification				O/S		x	x	x
AC-9	Previous Logon Notification				S				
AC-9(1)	Unsuccessful Logons				S				
AC-9(2)	Successful and Unsuccessful Logons				S				
AC-9(3)	Notification of Account Changes				S				
AC-9(4)	Additional Logon Information				S				
AC-10	Concurrent Session Control				S				x
AC-11	Device Lock				S			x	x
AC-11(1)	Pattern-Hiding Displays				S			x	x
AC-12	Session Termination				S			x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
AC-12(1)	User-Initiated Logouts				O/S				
AC-12(2)	Termination Message	x			S				
AC-12(3)	Timeout Warning Message	x			S				
AC-14	Permitted Actions without Identification or Authentication				O		x	x	x
AC-16	Security and Privacy Attributes		x		O				
AC-16(1)	Dynamic Attribute Association				S				
AC-16(2)	Attribute Value Changes by Authorized Individuals				S				
AC-16(3)	Maintenance of Attribute Associations by System				S				
AC-16(4)	Association of Attributes by Authorized Individuals				S				
AC-16(5)	Attribute Displays on Objects to be Output				S				
AC-16(6)	Maintenance of Attribute Association				O				
AC-16(7)	Consistent Attribute Interpretation				O				
AC-16(8)	Association Techniques and Technologies				S				
AC-16(9)	Attribute Reassignment – Regrading Mechanisms				O				
AC-16(10)	Attribute Configuration by Authorized Individuals				O				
AC-17	Remote Access				O		x	x	x
AC-17(1)	Monitoring and Control				O/S			x	x
AC-17(2)	Protection of Confidentiality and Integrity Using Encryption				S			x	x
AC-17(3)	Managed Access Control Points				S			x	x
AC-17(4)	Privileged Commands and Access				O			x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
AC-17(6)	Protection of Mechanism Information				O				
AC-17(9)	Disconnect or Disable Access				O				
AC-17(10)	Authenticate Remote Commands	x			S				
AC-18	Wireless Access				O		x	x	x
AC-18(1)	Authentication and Encryption				S			x	x
AC-18(3)	Disable Wireless Networking				O/S			x	x
AC-18(4)	Restrict Configurations by Users				O				x
AC-18(5)	Antennas and Transmission Power Levels				O				x
AC-19	Access Control for Mobile Devices				O		x	x	x
AC-19(4)	Restrictions for Classified Information				O				
AC-19(5)	Full Device or Container-Based Encryption				O			x	x
AC-20	Use of External Systems				O		x	x	x
AC-20(1)	Limits on Authorized Use				O			x	x
AC-20(2)	Portable Storage Devices — Restricted Use				O			x	x
AC-20(3)	Non-Organizationally Owned Systems — Restricted Use				O				
AC-20(4)	Network Accessible Storage Devices — Prohibited Use				O				
AC-20(5)	Portable Storage Devices — Prohibited Use	x			O				
AC-21	Information Sharing				O			x	x
AC-21(1)	Automated Decision Support				S				
AC-21(2)	Information Search and Retrieval				S				
AC-22	Publicly Accessible Content				O		x	x	x

ACCESS CONTROL (AC)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
AC-23	Data Mining Protection				O				
AC-24	Access Control Decisions				O				
AC-24(1)	Transmit Access Authorization Information				S				
AC-24(2)	No User or Process Identity				S				
AC-25	Reference Monitor				S				

AWARENESS AND TRAINING (AT)

AT-1	Policy and Procedures				O	x	x	x	x
AT-2	Literacy Training and Awareness				O	x	x	x	x
AT-2(1)	Practical Exercises				O				
AT-2(2)	Insider Threat				O		X	x	x
AT-2(3)	Social Engineering and Mining	x			O			x	x
AT-2(4)	Suspicious Communications and Anomalous System Behavior	x			O				
AT-2(5)	Advanced Persistent Threat	x			O				
AT-2(6)	Cyber Threat Environment	x			O				
AT-3	Role-Based Training				O	x	x	x	x
AT-3(1)	Environmental Controls				O				
AT-3(2)	Physical Security Controls				O				
AT-3(3)	Practical Exercises				O				
AT-3(4)	Suspicious Communications and Anomalous System Behavior			→ AT-2(4)					
AT-3(5)	Processing Personally Identifiable Information	x			O	x			
AT-4	Training Records				O	x	x	x	x
AT-6	Training Feedback	x			O				

AUDIT AND ACCOUNTABILITY (AU)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
AU-1	Policy and Procedures				O	x	x	x	x
AU-2	Event Logging		x		O	x	x	x	x
AU-2(3)	Reviews and Updates			→ AU-2					
AU-3	Content of Audit Records				S		x	x	x
AU-3(1)	Additional Audit Information				S			x	x
AU-3(2)	Centralized Management of Planned Audit Record Content			→ PL-9					
AU-3(3)	Limit Personally Identifiable Information Elements	x			O	x			
AU-4	Audit Log Storage Capacity				O/S		x	x	x
AU-4(1)	Transfer to Alternate Storage				O/S				
AU-5	Response to Audit Logging Process Failures				S		x	x	x
AU-5(1)	Storage Capacity Warning				S				x
AU-5(2)	Real-Time Alerts				S				x
AU-5(3)	Configurable Traffic Volume Thresholds				S				
AU-5(4)	Shutdown on Failure				S				
AU-5(5)	Alternate Audit Logging Capability	x			O				
AU-6	Audit Record Review, Analysis, and Reporting		x		O		x	x	x
AU-6(1)	Automated Process Integration				O			x	x
AU-6(3)	Correlate Audit Record Repositories				O			x	x
AU-6(4)	Central Review and Analysis				S				
AU-6(5)	Integrated Analysis of Audit Records				O				x
AU-6(6)	Correlation with Physical Monitoring				O				x
AU-6(7)	Permitted Actions				O				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
AU-6(8)	Full Text Analysis of Privileged Commands				O				
AU-6(9)	Correlation with Information from Nontechnical Sources				O				
AU-6(10)	Audit Level Adjustment			→ AU-6					
AU-7	Audit Record Reduction and Report Generation				S			x	x
AU-7(1)	Automatic Processing		x		S			x	x
AU-7(2)	Automatic Search and Sort			→ AU-7(1)					
AU-8	Time Stamps				S		x	x	x
AU-8(1)	Synchronization with Authoritative Time Source			→ SC-45(1)					
AU-8(2)	Secondary Authoritative Time Source			→ SC-45(2)					
AU-9	Protection of Audit Information				S		x	x	x
AU-9(1)	Hardware Write-Once Media				S				
AU-9(2)	Store on Separate Physical Systems or Components				S				x
AU-9(3)	Cryptographic Protection				S				x
AU-9(4)	Access by Subset of Privileged Users				O			x	x
AU-9(5)	Dual Authorization				O/S				
AU-9(6)	Read-Only Access				O/S				
AU-9(7)	Store on Component with Different Operating System	x			O				
AU-10	Non-repudiation				S				x
AU-10(1)	Association of Identities				S				
AU-10(2)	Validate Binding of Information Producer Identity				S				
AU-10(3)	Chain of Custody				O/S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
AU-10(4)	Validate Binding of Information Reviewer Identity				S				
AU-11	Audit Record Retention				O	x	x	x	x
AU-11(1)	Long-Term Retrieval Capability				O				
AU-12	Audit Record Generation				S		x	x	x
AU-12(1)	System-Wide and Time-Correlated Audit Trail				S				x
AU-12(2)	Standardized Formats				S				
AU-12(3)	Changes by Authorized Individuals				S				x
AU-12(4)	Query Parameter Audits of Personally Identifiable Information	x			S				
AU-13	Monitoring for Information Disclosure				O				
AU-13(1)	Use of Automated Tools				O/S				
AU-13(2)	Review of Monitored Sites				O				
AU-13(3)	Unauthorized Replication of Information	x			O/S				
AU-14	Session Audit		x		S				
AU-14(1)	System Start-Up				S				
AU-14(2)	Capture and Record Content			→ AU-14					
AU-14(3)	Remote Viewing and Listening				S				
AU-15	Alternate Audit Logging Capability			→ AU-5(5)					
AU-16	Cross-Organizational Audit Logging				O				
AU-16(1)	Identity Preservation				O				
AU-16(2)	Sharing of Audit Information				O				
AU-16(3)	Disassociability	x			O				

ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
CA-1	Policy and Procedures				O	x	x	x	x
CA-2	Control Assessments				O	x	x	x	x
CA-2(1)	Independent Assessors				O			x	x
CA-2(2)	Specialized Assessments				O				x
CA-2(3)	Leveraging Results from External Organizations				O				
CA-3	Information Exchange				O		x	x	x
CA-3(1)	Unclassified National Security Connections			→ SC-7(25)					
CA-3(2)	Classified National Security System Connections			→ SC-7(26)					
CA-3(3)	Unclassified Non-National Security System Connections			→ SC-7(27)					
CA-3(4)	Connections to Public Networks			→ SC-7(28)					
CA-3(5)	Restrictions on External System Connections			→ SC-7(5)					
CA-3(6)	Transfer Authorizations	x			O/S				x
CA-3(7)	Transitive Information Exchanges	x			O/S				
CA-5	Plan of Action and Milestones				O	x	x	x	x
CA-5(1)	Automation Support for Accuracy and Currency				O				
CA-6	Authorization				O	x	x	x	x
CA-6(1)	Joint Authorization — Intra-Organization	x			O				
CA-6(2)	Joint Authorization — Inter-Organization	x			O				
CA-7	Continuous Monitoring				O	x	x	x	x
CA-7(1)	Independent Assessment				O			x	x
CA-7(3)	Trend Analyses				O				
CA-7(4)	Risk Monitoring	x			O/S	x	x	x	x

ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
CA-7(5)	Consistency Analysis	x			O				
CA-7(6)	Automation Support for Monitoring	x			O/S				
CA-8	Penetration Testing		x		O				x
CA-8(1)	Independent Penetration Testing Agent or Team				O				x
CA-8(2)	Red Team Exercises				O				
CA-8(3)	Facility Penetration Testing	x			O				
CA-9	Internal System Connections				O		x	x	x
CA-9(1)	Compliance Checks				O/S				

CONFIGURATION MANAGEMENT (CM)

CM-1	Policy and Procedures				O	x	x	x	x
CM-2	Baseline Configuration		x		O		x	x	x
CM-2(1)	Reviews and Updates			→ CM-2					
CM-2(2)	Automation Support for Accuracy and Currency				O			x	x
CM-2(3)	Retention of Previous Configurations				O			x	x
CM-2(6)	Development and Test Environments				O				
CM-2(7)	Configure Systems and Components for High-Risk Areas				O			x	x
CM-3	Configuration Change Control				O			x	x
CM-3(1)	Automated Documentation, Notification, and Prohibition of Changes				O				x
CM-3(2)	Testing, Validation, and Documentation of Changes				O			x	x
CM-3(3)	Automated Change Implementation				O				

CONFIGURATION MANAGEMENT (CM)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
CM-3(4)	Security and Privacy Representatives				O			x	x
CM-3(5)	Automated Security Response				S				
CM-3(6)	Cryptography Management				O				x
CM-3(7)	Review System Changes	x			O				
CM-3(8)	Prevent or Restrict Configuration Changes	x			S				
CM-4	Impact Analyses				O	x	x	x	x
CM-4(1)	Separate Test Environments				O				x
CM-4(2)	Verification of Controls				O			x	x
CM-5	Access Restrictions for Change				O		x	x	x
CM-5(1)	Automated Access Enforcement and Audit Records				S				x
CM-5(2)	Review System Changes			→ CM-3(7)					
CM-5(3)	Signed Components			→ CM-14					
CM-5(4)	Dual Authorization				O/S				
CM-5(5)	Privilege Limitation for Production and Operation				O				
CM-5(6)	Limit Library Privileges				O/S				
CM-6	Configuration Settings				O/S		x	x	x
CM-6(1)	Automated Management, Application, and Verification				O				x
CM-6(2)	Respond to Unauthorized Changes				O				x
CM-7	Least Functionality				O/S		x	x	x
CM-7(1)	Periodic Review				O/S			x	x
CM-7(2)	Prevent Program Execution				S			x	x
CM-7(3)	Registration Compliance				O				
CM-7(4)	Unauthorized Software				O/S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
CM-7(5)	Authorized Software				O/S			x	x
CM-7(6)	Confined Environments with Limited Privileges	x			O				
CM-7(7)	Code Execution in Protected Environments	x			O/S				
CM-7(8)	Binary or Machine Executable Code	x			O/S				
CM-7(9)	Prohibiting the Use of Unauthorized Hardware	x			O/S				
CM-8	System Component Inventory		x		O		x	x	x
CM-8(1)	Updates During Installation and Removal				O			x	x
CM-8(2)	Automated Maintenance				O				x
CM-8(3)	Automated Unauthorized Component Detection		x		O			x	x
CM-8(4)	Accountability Information				O				x
CM-8(5)	No Duplicate Accounting of Components			→ CM-8					
CM-8(6)	Assessed Configurations and Approved Deviations				O				
CM-8(7)	Centralized Repository				O				
CM-8(8)	Automated Location Tracking				O				
CM-8(9)	Assignment of Components to Systems				O				
CM-9	Configuration Management Plan				O			x	x
CM-9(1)	Assignment of Responsibility				O				
CM-10	Software Usage Restrictions				O		x	x	x
CM-10(1)	Open-Source Software				O				
CM-11	User-Installed Software				O		x	x	x
CM-11(1)	Alerts for Unauthorized Installations			→ CM-8(3)					

CONFIGURATION MANAGEMENT (CM)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
CM-11(2)	Software Installation with Privileged Status				S				
CM-11(3)	Automated Enforcement and Monitoring	x			S				
CM-12	Information Location	x			O			x	x
CM-12(1)	Automated Tools to Support Information Location	x			O			x	x
CM-13	Data Action Mapping	x			O				
CM-14	Signed Components	x			O/S				

CONTINGENCY PLANNING (CP)

CP-1	Policy and Procedures				O		x	x	x
CP-2	Contingency Plan				O		x	x	x
CP-2(1)	Coordinate with Related Plans				O			x	x
CP-2(2)	Capacity Planning				O				x
CP-2(3)	Resume Mission and Business Functions		x		O			x	x
CP-2(4)	Resume all Mission and Business Functions			→ CP-2(3)					
CP-2(5)	Continue Mission and Business Functions				O				x
CP-2(6)	Alternate Processing and Storage Sites				O				
CP-2(7)	Coordinate with External Service Providers				O				
CP-2(8)	Identify Critical Assets				O			x	x
CP-3	Contingency Training				O		x	x	x
CP-3(1)	Simulated Events				O				x
CP-3(2)	Mechanisms Used in Training Environments				O				
CP-4	Contingency Plan Testing				O		x	x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
CP-4(1)	Coordinate with Related Plans				O			x	x
CP-4(2)	Alternate Processing Site				O				x
CP-4(3)	Automated Testing				O				
CP-4(4)	Full Recovery and Reconstitution				O				
CP-4(5)	Self-Challenge	x			O/S				
CP-6	Alternate Storage Site				O			x	x
CP-6(1)	Separation from Primary Site				O			x	x
CP-6(2)	Recovery Time and Recovery Point Objectives				O				x
CP-6(3)	Accessibility				O			x	x
CP-7	Alternate Processing Site				O			x	x
CP-7(1)	Separation from Primary Site				O			x	x
CP-7(2)	Accessibility				O			x	x
CP-7(3)	Priority of Service				O			x	x
CP-7(4)	Preparation for Use				O				x
CP-7(6)	Inability to Return to Primary Site				O				
CP-8	Telecommunications Services				O			x	x
CP-8(1)	Priority of Service Provisions				O			x	x
CP-8(2)	Single Points of Failure				O			x	x
CP-8(3)	Separation of Primary and Alternate Providers				O				x
CP-8(4)	Provider Contingency Plan				O				x
CP-8(5)	Alternate Telecommunication Service Testing				O				
CP-9	System Backup				O		x	x	x
CP-9(1)	Testing for Reliability and Integrity				O			x	x
CP-9(2)	Test Restoration Using Sampling				O				x

CONTINGENCY PLANNING (CP)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
CP-9(3)	Separate Storage for Critical Information				O				x
CP-9(5)	Transfer to Alternate Storage Site				O				x
CP-9(6)	Redundant Secondary System				O				
CP-9(7)	Dual Authorization				O				
CP-9(8)	Cryptographic Protection	x			O			x	x
CP-10	System Recovery and Reconstitution				O		x	x	x
CP-10(2)	Transaction Recovery				O			x	x
CP-10(4)	Restore Within Time Period				O				x
CP-10(6)	Component Protection				O				
CP-11	Alternate Communications Protocols				O				
CP-12	Safe Mode				S				
CP-13	Alternative Security Mechanisms				O/S				

IDENTIFICATION AND AUTHENTICATION (IA)

IA-1	Policy and Procedures				O		x	x	x
IA-2	Identification and Authentication (Organizational Users)				O/S		x	x	x
IA-2(1)	Multi-Factor Authentication to Privileged Accounts		x		S		x	x	x
IA-2(2)	Multi-Factor Authentication to Non-Privileged Accounts		x		S		x	x	x
IA-2(3)	Local Access to Privileged Accounts			→ IA-2(1)					
IA-2(4)	Local Access to Non-Privileged Accounts			→ IA-2(2)					
IA-2(5)	Individual Authentication with Group Authentication				O/S				x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
IA-2(6)	Access to Accounts — Separate Device		x		S				
IA-2(7)	Network Access to Non-Privileged Accounts — Separate Device			→ IA-2(6)					
IA-2(8)	Access to Accounts — Replay Resistant		x		S		x	x	x
IA-2(9)	Network Access to Non-Privileged Accounts — Replay Resistant			→ IA-2(8)					
IA-2(10)	Single Sign-On				S				
IA-2(11)	Remote Access — Separate Device			→ IA-2(6)					
IA-2(12)	Acceptance of PIV Credentials				S		x	x	x
IA-2(13)	Out-of-Band Authentication				S				
IA-3	Device Identification and Authentication				S			x	x
IA-3(1)	Cryptographic Bidirectional Authentication				S				
IA-3(3)	Dynamic Address Allocation				O				
IA-3(4)	Device Attestation				O				
IA-4	Identifier Management				O		x	x	x
IA-4(1)	Prohibit Account Identifiers as Public Identifiers				O				
IA-4(2)	Supervisor Authorization			→ IA-12(1)					
IA-4(3)	Multiple Forms of Certification			→ IA-12(2)					
IA-4(4)	Identify User Status				O			x	x
IA-4(5)	Dynamic Management				S				
IA-4(6)	Cross-Organization Management				O				
IA-4(7)	In-Person Registration			→ IA-12(4)					
IA-4(8)	Pairwise Pseudonymous Identifiers	x			O				
IA-4(9)	Attribute Maintenance and Protection	x			O/S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
IA-5	Authenticator Management				O/S		x	x	x
IA-5(1)	Password-Based Authentication		x		O/S		x	x	x
IA-5(2)	Public Key-Based Authentication				S			x	x
IA-5(3)	In-Person or Trusted External Party Registration			→ IA-12(4)					
IA-5(4)	Automated Support for Password Strength Determination			→ IA-5(1)					
IA-5(5)	Change Authenticators Prior to Delivery				O				
IA-5(6)	Protection of Authenticators				O			x	x
IA-5(7)	No Embedded Unencrypted Static Authenticators				O				
IA-5(8)	Multiple System Accounts				O				
IA-5(9)	Federated Credential Management				O				
IA-5(10)	Dynamic Credential Binding				S				
IA-5(11)	Hardware Token-Based Authentication			→ IA-2(1)(2)					
IA-5(12)	Biometric Authentication Performance				S				
IA-5(13)	Expiration of Cached Authenticators				S				
IA-5(14)	Managing Content of PKI Trust Stores				O				
IA-5(15)	GSA-Approved Products and Services				O				
IA-5(16)	In-Person or Trusted External Party Authenticator Issuance	x			O				
IA-5(17)	Presentation Attack Detection for Biometric Authenticators	x			S				
IA-5(18)	Password Managers	x			S				
IA-6	Authentication Feedback				S		x	x	x
IA-7	Cryptographic Module Authentication				S		x	x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
IA-8	Identification and Authentication (Non-Organizational Users)				S		x	x	x
IA-8(1)	Acceptance of PIV Credentials from Other Agencies				S		x	x	x
IA-8(2)	Acceptance of External Authenticators		x		S		x	x	x
IA-8(3)	Use of FICAM-Approved Products			→ IA-8(2)					
IA-8(4)	Use of Defined Profiles				S		x	x	x
IA-8(5)	Acceptance of PIV-I Credentials				S				
IA-8(6)	Disassociability	x			O				
IA-9	Service Identification and Authentication		x		O/S				
IA-9(1)	Information Exchange			→ IA-9					
IA-9(2)	Transmission of Decisions			→ IA-9					
IA-10	Adaptive Authentication				O				
IA-11	Re-authentication				O/S		x	x	x
IA-12	Identity Proofing	x			O			x	x
IA-12(1)	Supervisor Authorization	x			O				
IA-12(2)	Identity Evidence	x			O			x	x
IA-12(3)	Identity Evidence Validation and Verification	x			O			x	x
IA-12(4)	In-Person Validation and Verification	x			O				x
IA-12(5)	Address Confirmation	x			O			x	x
IA-12(6)	Accept Externally-Proofed Identities	x			O				

INCIDENT RESPONSE (IR)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
IR-1	Policy and Procedures				O	x	x	x	x
IR-2	Incident Response Training				O	x	x	x	x
IR-2(1)	Simulated Events				O				x
IR-2(2)	Automated Training Environments				O				x
IR-2(3)	Breach	x			O	x			
IR-3	Incident Response Testing				O	x		x	x
IR-3(1)	Automated Testing				O				
IR-3(2)	Coordination with Related Plans				O			x	x
IR-3(3)	Continuous Improvement	x			O				
IR-4	Incident Handling				O	x	x	x	x
IR-4(1)	Automated Incident Handling Processes				O			x	x
IR-4(2)	Dynamic Reconfiguration				O				
IR-4(3)	Continuity of Operations				O				
IR-4(4)	Information Correlation				O				x
IR-4(5)	Automatic Disabling of System				O/S				
IR-4(6)	Insider Threats				O				
IR-4(7)	Insider Threats — Intra-Organization Coordination				O				
IR-4(8)	Correlation with External Organizations				O				
IR-4(9)	Dynamic Response Capability				O				
IR-4(10)	Supply Chain Coordination				O				
IR-4(11)	Integrated Incident Response Team	x			O				x
IR-4(12)	Malicious Code and Forensic Analysis	x			O				
IR-4(13)	Behavior Analysis	x			O				
IR-4(14)	Security Operations Center	x			O/S				

INCIDENT RESPONSE (IR)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
IR-4(15)	Public Relations and Reputation Repair	x			O				
IR-5	Incident Monitoring				O	x	x	x	x
IR-5(1)	Automated Tracking, Data Collection, and Analysis				O				x
IR-6	Incident Reporting				O	x	x	x	x
IR-6(1)	Automated Reporting				O			x	x
IR-6(2)	Vulnerabilities Related to Incidents				O				
IR-6(3)	Supply Chain Coordination				O			x	x
IR-7	Incident Response Assistance				O	x	x	x	x
IR-7(1)	Automation Support for Availability of Information and Support				O			x	x
IR-7(2)	Coordination with External Providers				O				
IR-8	Incident Response Plan				O	x	x	x	x
IR-8(1)	Breaches	x			O	x			
IR-9	Information Spillage Response		x		O				
IR-9(1)	Responsible Personnel			→ IR-9					
IR-9(2)	Training				O				
IR-9(3)	Post-Spill Operations				O				
IR-9(4)	Exposure to Unauthorized Personnel				O				
IR-10	Integrated Information Security Analysis			→ IR-4(11)					

MAINTENANCE (MA)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
MA-1	Policy and Procedures		x		O		x	x	x
MA-2	Controlled Maintenance				O		x	x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
MA-2(2)	Automated Maintenance Activities				O				x
MA-3	Maintenance Tools				O			x	x
MA-3(1)	Inspect Tools				O			x	x
MA-3(2)	Inspect Media				O			x	x
MA-3(3)	Prevent Unauthorized Removal				O			x	x
MA-3(4)	Restricted Tool Use				O/S				
MA-3(5)	Execution with Privilege	x			O/S				
MA-3(6)	Software Updates and Patches	x			O/S				
MA-4	Nonlocal Maintenance		x		O		x	x	x
MA-4(1)	Logging and Review				O				
MA-4(2)	Document Nonlocal Maintenance			→ MA-1, MA-4					
MA-4(3)	Comparable Security and Sanitization				O				x
MA-4(4)	Authentication and Separation of Maintenance Sessions				O				
MA-4(5)	Approvals and Notifications				O				
MA-4(6)	Cryptographic Protection				O/S				
MA-4(7)	Disconnect Verification				S				
MA-5	Maintenance Personnel				O		x	x	x
MA-5(1)	Individuals without Appropriate Access				O				x
MA-5(2)	Security Clearances for Classified Systems				O				
MA-5(3)	Citizenship Requirements for Classified Systems				O				
MA-5(4)	Foreign Nationals				O				
MA-5(5)	Non-System Maintenance				O				
MA-6	Timely Maintenance		x		O			x	x
MA-6(1)	Preventive Maintenance				O				

MAINTENANCE (MA)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
MA-6(2)	Predictive Maintenance				O				
MA-6(3)	Automated Support for Predictive Maintenance				O				
MA-7	Field Maintenance	x			O				

MEDIA PROTECTION (MP)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
MP-1	Policy and Procedures				O	x	x	x	x
MP-2	Media Access				O		x	x	x
MP-3	Media Marking				O			x	x
MP-4	Media Storage				O			x	x
MP-4(2)	Automated Restricted Access				O				
MP-5	Media Transport				O			x	x
MP-5(3)	Custodians				O				
MP-5(4)	Cryptographic Protection			→ SC-28(1)					
MP-6	Media Sanitization				O	x	x	x	x
MP-6(1)	Review, Approve, Track, Document, and Verify				O				x
MP-6(2)	Equipment Testing				O				x
MP-6(3)	Nondestructive Techniques				O				x
MP-6(7)	Dual Authorization				O				
MP-6(8)	Remote Purging or Wiping of Information				O				
MP-7	Media Use		x		O		x	x	x
MP-7(1)	Prohibit Use without Owner			→ MP-7					
MP-7(2)	Prohibit Use of Sanitization-Resistant Media				O				
MP-8	Media Downgrading				O				
MP-8(1)	Documentation of Process				O				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
MP-8(2)	Equipment Testing				O				
MP-8(3)	Controlled Unclassified Information				O				
MP-8(4)	Classified Information				O				

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
PE-1	Policy and Procedures				O		x	x	X
PE-2	Physical Access Authorizations				O		x	x	x
PE-2(1)	Access by Position and Role				O				
PE-2(2)	Two Forms of Identification				O				
PE-2(3)	Restrict Unescorted Access				O				
PE-3	Physical Access Control				O		x	x	x
PE-3(1)	System Access				O				x
PE-3(2)	Facility and Systems				O				
PE-3(3)	Continuous Guards				O				
PE-3(4)	Lockable Casings				O				
PE-3(5)	Tamper Protection				O				
PE-3(6)	Facility Penetration Testing			→ CA-8					
PE-3(7)	Physical Barriers	x			O				
PE-3(8)	Access Control Vestibules	x			O				
PE-4	Access Control for Transmission				O			x	x
PE-5	Access Control for Output Devices		x		O			x	x
PE-5(1)	Access to Output by Authorized Individuals			→ PE-5					
PE-5(2)	Link to Individual Identity				S				
PE-5(3)	Marking Output Devices			→ PE-22					
PE-6	Monitoring Physical Access				O		x	x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
PE-6(1)	Intrusion Alarms and Surveillance Equipment				O			x	x
PE-6(2)	Automated Intrusion Recognition and Responses				O				
PE-6(3)	Video Surveillance				O				
PE-6(4)	Monitoring Physical Access to Systems				O				x
PE-8	Visitor Access Records				O		x	x	x
PE-8(1)	Automated Records Maintenance and Review				O				x
PE-8(3)	Limit Personally Identifiable Information Elements	x			O	x			
PE-9	Power Equipment and Cabling				O			x	x
PE-9(1)	Redundant Cabling				O				
PE-9(2)	Automatic Voltage Controls				O				
PE-10	Emergency Shutoff				O			x	x
PE-11	Emergency Power				O			x	x
PE-11(1)	Alternate Power Supply — Minimal Operational Capability				O				x
PE-11(2)	Alternate Power Supply — Self-Contained				O				
PE-12	Emergency Lighting				O		x	x	x
PE-12(1)	Essential Mission and Business Functions				O				
PE-13	Fire Protection				O		x	x	x
PE-13(1)	Detection Systems — Automatic Activation and Notification				O			x	x
PE-13(2)	Suppression Systems — Automatic Activation and Notification		x		O				x
PE-13(3)	Automatic Fire Suppression			→ PE-13(2)					
PE-13(4)	Inspections				O				

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
PE-14	Environmental Controls				O		x	x	x
PE-14(1)	Automatic Controls				O				
PE-14(2)	Monitoring with Alarms and Notifications				O				
PE-15	Water Damage Protection				O		x	x	x
PE-15(1)	Automation Support				O				x
PE-16	Delivery and Removal				O		x	x	x
PE-17	Alternate Work Site				O			x	x
PE-18	Location of System Components				O				x
PE-18(1)	Location of System Components / Facility Site			→ PE-23					
PE-19	Information Leakage				O				
PE-19(1)	National Emissions and Tempest Policies and Procedures				O				
PE-20	Asset Monitoring and Tracking				O				
PE-21	Electromagnetic Pulse Protection	x			O				
PE-22	Component Marking	x			O				
PE-23	Facility Location	x			O				

PLANNING (PL)

PL-1	Policy and Procedures				O	x	x	x	x
PL-2	System Security and Privacy Plans		x		O	x	x	x	x
PL-2(3)	Plan and Coordinate with Other Organizational Entities			→ PL-2					
PL-4	Rules of Behavior				O	x	x	x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
PL-4(1)	Social Media and External Site/Application Usage Restrictions				O	x	x	x	x
PL-7	Concept of Operations				O				
PL-8	Security and Privacy Architectures				O	x		x	x
PL-8(1)	Defense in Depth				O				
PL-8(2)	Supplier Diversity				O				
PL-9	Central Management		x		O	x			
PL-10	Baseline Selection	x			O		x	x	x
PL-11	Baseline Tailoring	x			O		x	x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
PM-1	Information Security Program Plan				O		x	x	x
PM-2	Information Security Program Leadership Role				O		x	x	x
PM-3	Information Security and Privacy Resources				O	x	x	x	x
PM-4	Plan of Action and Milestones Process				O	x	x	x	x
PM-5	System Inventory				O		x	x	x
PM-5(1)	Inventory of Personally Identifiable Information	x			O	x	x	x	x
PM-6	Measures of Performance				O	x	x	x	x
PM-7	Enterprise Architecture				O	x	x	x	x
PM-7(1)	Offloading	x			O		x	x	x
PM-8	Critical Infrastructure Plan				O	x	x	x	x
PM-9	Risk Management Strategy				O	x	x	x	x
PM-10	Authorization Process				O	x	x	x	x
PM-11	Mission and Business Process Definition				O	x	x	x	x
PM-12	Insider Threat Program				O		x	x	x
PM-13	Security and Privacy Workforce				O	x	x	x	x
PM-14	Testing, Training, and Monitoring				O	x	x	x	x
PM-15	Security and Privacy Groups and Associations				O		x	x	x
PM-16	Threat Awareness Program				O		x	x	x
PM-16(1)	Automated Means for Sharing Threat Intelligence	x			O		x	x	x
PM-17	Protecting Controlled Unclassified Information on External Systems	x			O	x	x	x	x
PM-18	Privacy Program Plan	x			O	x	x	x	x
PM-19	Privacy Program Leadership Role	x			O	x	x	x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
PM-20	Dissemination of Privacy Program Information	x			O	x	x	x	x
PM-20(1)	Privacy Policies on Websites, Applications, and Digital Services	x			O	x	x	x	x
PM-21	Accounting of Disclosures	x			O	x	x	x	x
PM-22	Personally Identifiable Information Quality Management	x			O	x	x	x	x
PM-23	Data Governance Body	x			O		x	x	x
PM-24	Data Integrity Board	x			O	x	x	x	x
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	x			O	x	x	x	x
PM-26	Complaint Management	x			O	x	x	x	x
PM-27	Privacy Reporting	x			O	x	x	x	x
PM-28	Risk Framing	x			O	x	x	x	x
PM-29	Risk Management Program Leadership Roles	x			O		x	x	x
PM-30	Supply Chain Risk Management Strategy	x			O		x	x	x
PM-30(1)	Suppliers of Critical or Mission-Essential Items	x			O		x	x	x
PM-31	Continuous Monitoring Strategy	x			O	x	x	x	x
PM-32	Purposing	x			O		x	x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
PS-1	Policy and Procedures				O		x	x	x
PS-2	Position Risk Designation				O		x	x	x
PS-3	Personnel Screening				O		x	x	x
PS-3(1)	Classified Information				O				
PS-3(2)	Formal Indoctrination				O				
PS-3(3)	Information with Special Protection Measures				O				
PS-3(4)	Citizenship Requirements	x			O				
PS-4	Personnel Termination				O		x	x	x
PS-4(1)	Post-Employment Requirements				O				
PS-4(2)	Automated Actions				O				x
PS-5	Personnel Transfer				O		x	x	x
PS-6	Access Agreements				O	x	x	x	x
PS-6(2)	Classified Information Requiring Special Protection				O				
PS-6(3)	Post-Employment Requirements				O				
PS-7	External Personnel Security				O		x	x	x
PS-8	Personnel Sanctions				O		x	x	x
PS-9	Position Descriptions	x			O		x	x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
PT-1	Policy and Procedures (PII Processing and Transparency)	x			O	x			
PT-2	Authority to Process Personally Identifiable Information	x			O	x			
PT-2(1)	Data Tagging	x			S	x			
PT-2(2)	Automation	x			O	x			
PT-3	Personally Identifiable Information Processing Purposes	x			O	x			
PT-3(1)	Data Tagging	x			S	x			
PT-3(2)	Automation	x			O	x			
PT-4	Consent	x			O	x			
PT-4(1)	Tailored Consent	x			O	x			
PT-4(2)	Just-in-Time Consent	x			O	x			
PT-4(3)	Revocation	x			O	x			
PT-5	Privacy Notice	x			O	x			
PT-5(1)	Just-in-Time Notice	x			O	x			
PT-5(2)	Privacy Act Statements	x			O	x			
PT-6	System of Records Notice	x			O	x			
PT-6(1)	Routine Uses	x			O	x			
PT-6(2)	Exemption Rules	x			O	x			
PT-7	Specific Categories of Personally Identifiable Information	x			O	x			
PT-7(1)	Social Security Numbers	x			O	x			
PT-7(2)	First Amendment Information	x			O	x			
PT-8	Computer Matching Requirements	x			O	x			

RISK ASSESSMENT (RA)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
RA-1	Policy and Procedures				O	x	x	x	x
RA-2	Security Categorization				O		x	x	x
RA-2(1)	Impact-Level Prioritization	x			O				
RA-3	Risk Assessment				O	x	x	x	x
RA-3(1)	Supply Chain Risk Assessment	x			O		x	x	x
RA-3(2)	Use of All-Source Intelligence	x			O				
RA-3(3)	Dynamic Threat Awareness	x			O				
RA-3(4)	Predictive Cyber Analytics	x			O				
RA-5	Vulnerability Monitoring and Scanning		x		O		x	x	x
RA-5(1)	Update Tool Capability			→ RA-5					
RA-5(2)	Update Vulnerabilities to be Scanned				O		x	x	x
RA-5(3)	Breadth and Depth of Coverage				O				
RA-5(4)	Discoverable Information				O				x
RA-5(5)	Privileged Access				O			x	x
RA-5(6)	Automated Trend Analyses				O				
RA-5(8)	Review Historic Audit Logs				O				
RA-5(10)	Correlate Scanning Information				O				
RA-5(11)	Public Disclosure Program	x			O		x	x	x
RA-6	Technical Surveillance Countermeasures Survey				O				
RA-7	Risk Response	x			O	x	x	x	x
RA-8	Privacy Impact Assessments	x			O	x			
RA-9	Criticality Analysis	x			O			x	x
RA-10	Threat Hunting	x			O/S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SA-1	Policy and Procedures				O	x	x	x	x
SA-2	Allocation of Resources				O	x	x	x	x
SA-3	System Development Life Cycle				O	x	x	x	x
SA-3(1)	Manage Preproduction Environment	x			O				
SA-3(2)	Use of Live or Operational Data	x			O				
SA-3(3)	Technology Refresh	x			O				
SA-4	Acquisition Process				O	x	x	x	x
SA-4(1)	Functional Properties of Controls				O			x	x
SA-4(2)	Design and Implementation Information for Controls				O			x	x
SA-4(3)	Development Methods, Techniques, and Practices				O				
SA-4(5)	System, Component, and Service Configurations				O				x
SA-4(6)	Use of Information Assurance Products				O				
SA-4(7)	NIAP-Approved Protection Profiles				O				
SA-4(8)	Continuous Monitoring Plan for Controls				O				
SA-4(9)	Functions, Ports, Protocols, and Services in Use				O			x	x
SA-4(10)	Use of Approved PIV Products				O		x	x	x
SA-4(11)	System of Records	x			O				
SA-4(12)	Data Ownership	x			O				
SA-5	System Documentation				O		x	x	x
SA-8	Security and Privacy Engineering Principles		x		O		x	x	x
SA-8(1)	Clear Abstractions	x			O/S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SA-8(2)	Least Common Mechanism	x			O/S				
SA-8(3)	Modularity and Layering	x			O/S				
SA-8(4)	Partially Ordered Dependencies	x			O/S				
SA-8(5)	Efficiently Mediated Access	x			O/S				
SA-8(6)	Minimized Sharing	x			O/S				
SA-8(7)	Reduced Complexity	x			O/S				
SA-8(8)	Secure Evolvability	x			O/S				
SA-8(9)	Trusted Components	x			O/S				
SA-8(10)	Hierarchical Trust	x			O/S				
SA-8(11)	Inverse Modification Threshold	x			O/S				
SA-8(12)	Hierarchical Protection	x			O/S				
SA-8(13)	Minimized Security Elements	x			O/S				
SA-8(14)	Least Privilege	x			O/S				
SA-8(15)	Predicate Permission	x			O/S				
SA-8(16)	Self-Reliant Trustworthiness	x			O/S				
SA-8(17)	Secure Distributed Composition	x			O/S				
SA-8(18)	Trusted Communications Channels	x			O/S				
SA-8(19)	Continuous Protection	x			O/S				
SA-8(20)	Secure Metadata Management	x			O/S				
SA-8(21)	Self-Analysis	x			O/S				
SA-8(22)	Accountability and Traceability	x			O/S				
SA-8(23)	Secure Defaults	x			O/S				
SA-8(24)	Secure Failure and Recovery	x			O/S				
SA-8(25)	Economic Security	x			O/S				
SA-8(26)	Performance Security	x			O/S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SA-8(27)	Human Factored Security	x			O/S				
SA-8(28)	Acceptable Security	x			O/S				
SA-8(29)	Repeatable and Documented Procedures	x			O/S				
SA-8(30)	Procedural Rigor	x			O/S				
SA-8(31)	Secure System Modification	x			O/S				
SA-8(32)	Sufficient Documentation	x			O/S				
SA-8(33)	Minimization	x			O/S	x			
SA-9	External System Services				O	x	x	x	x
SA-9(1)	Risk Assessments and Organizational Approvals				O				
SA-9(2)	Identification of Functions, Ports, Protocols, and Services				O			x	x
SA-9(3)	Establish and Maintain Trust Relationship with Providers				O				
SA-9(4)	Consistent Interests of Consumers and Providers				O				
SA-9(5)	Processing, Storage, and Service Location				O				
SA-9(6)	Organization-Controlled Cryptographic Keys	x			O				
SA-9(7)	Organization-Controlled Integrity Checking	x			O				
SA-9(8)	Processing and Storage Location — US Jurisdiction	x			O				
SA-10	Developer Configuration Management				O			x	x
SA-10(1)	Software and Firmware Integrity Verification				O				
SA-10(2)	Alternative Configuration Management Processes				O				
SA-10(3)	Hardware Integrity Verification				O				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SA-10(4)	Trusted Generation				O				
SA-10(5)	Mapping Integrity for Version Control				O				
SA-10(6)	Trusted Distribution				O				
SA-10(7)	Security and Privacy Representatives	x			O				
SA-11	Developer Testing and Evaluation				O	x		x	x
SA-11(1)	Static Code Analysis				O				
SA-11(2)	Threat Modeling and Vulnerability Analyses		x		O				
SA-11(3)	Independent Verification of Assessment Plans and Evidence				O				
SA-11(4)	Manual Code Reviews				O				
SA-11(5)	Penetration Testing				O				
SA-11(6)	Attack Surface Reviews				O				
SA-11(7)	Verify Scope of Testing and Evaluation				O				
SA-11(8)	Dynamic Code Analysis				O				
SA-11(9)	Interactive Application Security Testing	x			O				
SA-12	Supply Chain Protection			→ SR Family					
SA-12(1)	Acquisition Strategies, Tools, and Methods			→ SR-5					
SA-12(2)	Supplier Reviews			→ SR-6					
SA-12(3)	Trusted Shipping and Warehousing			→ SR-3					
SA-12(4)	Diversity of Suppliers			→ SR-3(1)					
SA-12(5)	Limitation of Harm			→ SR-3(2)					
SA-12(6)	Minimizing Procurement Time			→ SR-5(1)					

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SA-12(7)	Assessments Prior to Selection / Acceptance / Update			→ SR-5(2)					
SA-12(8)	Use of All-Source Intelligence			→ RA-3(2)					
SA-12(9)	Operations Security			→ SR-7					
SA-12(10)	Validate as Genuine and Not Altered			→ SR-4(3)					
SA-12(11)	Penetration Testing / Analysis of Elements, Processes, and Actors			→ SR-6(1)					
SA-12(12)	Inter-Organizational Agreements			→ SR-8					
SA-12(13)	Critical Information System Components			→ MA-6, RA-9					
SA-12(14)	Identity and Traceability			→ SR-4(1)(2)					
SA-12(15)	Process to Address Weaknesses or Deficiencies			→ SR-3					
SA-13	Trustworthiness			→ SA-8					
SA-14	Criticality Analysis			→ RA-9					
SA-15	Development Process, Standards, and Tools				O			x	x
SA-15(1)	Quality Metrics				O				
SA-15(2)	Security and Privacy Tracking Tools				O				
SA-15(3)	Criticality Analysis				O			x	x
SA-15(4)	Threat Modeling and Vulnerability Analysis			→ SA-11(2)					
SA-15(5)	Attack Surface Reduction				O				
SA-15(6)	Continuous Improvement				O				
SA-15(7)	Automated Vulnerability Analysis				O				
SA-15(8)	Reuse of Threat and Vulnerability Information				O				
SA-15(9)	Use of Live Data			→ SA-3(2)					

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SA-15(10)	Incident Response Plan				O				
SA-15(11)	Archive System or Component				O				
SA-15(12)	Minimize Personally Identifiable Information	x			O				
SA-16	Developer-Provided Training				O				x
SA-17	Developer Security and Privacy Architecture and Design				O				x
SA-17(1)	Formal Policy Model				O				
SA-17(2)	Security-Relevant Components				O				
SA-17(3)	Formal Correspondence				O				
SA-17(4)	Informal Correspondence				O				
SA-17(5)	Conceptually Simple Design				O				
SA-17(6)	Structure for Testing				O				
SA-17(7)	Structure for Least Privilege				O				
SA-17(8)	Orchestration	x			O				
SA-17(9)	Design Diversity	x			O				
SA-18	Tamper Resistance and Detection			→ SR-9					
SA-18(1)	Multiple Phases of System Development Life Cycle			→ SR-9(1)					
SA-18(2)	Inspection of Systems or Components			→ SR-10					
SA-19	Component Authenticity			→ SR-11					
SA-19(1)	Anti-Counterfeit Training			→ SR-11(1)					
SA-19(2)	Configuration Control for Component Service and Repair			→ SR-11(2)					
SA-19(3)	Component Disposal			→ SR-12					
SA-19(4)	Anti-Counterfeit Scanning			→ SR-11(3)					
SA-20	Customized Development of Critical Components				O				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SA-21	Developer Screening		x		O				x
SA-21(1)	Validation of Screening			→ SA-21					
SA-22	Unsupported System Components		x		O		x	x	x
SA-22(1)	Alternative Sources for Continued Support			→ SA-22					
SA-23	Specialization	x			O				
SC-1	Policy and Procedures				O		x	x	x
SC-2	Separation of System and User Functionality				S			x	x
SC-2(1)	Interfaces for Non-Privileged Users				S				
SC-2(2)	Disassociability	x			S				
SC-3	Security Function Isolation				S				x
SC-3(1)	Hardware Separation				S				
SC-3(2)	Access and Flow Control Functions				S				
SC-3(3)	Minimize Nonsecurity Functionality				O/S				
SC-3(4)	Module Coupling and Cohesiveness				O/S				
SC-3(5)	Layered Structures				O/S				
SC-4	Information in Shared System Resources				S			x	x
SC-4(2)	Multilevel or Periods Processing				S				
SC-5	Denial-of-Service Protection				S		x	x	x
SC-5(1)	Restrict Ability to Attack Other Systems				S				
SC-5(2)	Capacity, Bandwidth, and Redundancy				S				
SC-5(3)	Detection and Monitoring				S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SC-6	Resource Availability				S				
SC-7	Boundary Protection				S		x	x	x
SC-7(3)	Access Points				S			x	x
SC-7(4)	External Telecommunications Services				O			x	x
SC-7(5)	Deny by Default — Allow by Exception		x		S			x	x
SC-7(7)	Split Tunneling for Remote Devices				S			x	x
SC-7(8)	Route Traffic to Authenticated Proxy Servers				S			x	x
SC-7(9)	Restrict Threatening Outgoing Communications Traffic				S				
SC-7(10)	Prevent Exfiltration				S				
SC-7(11)	Restrict Incoming Communications Traffic				S				
SC-7(12)	Host-Based Protection				S				
SC-7(13)	Isolation of Security Tools, Mechanisms, and Support Components				S				
SC-7(14)	Protect Against Unauthorized Physical Connections				S				
SC-7(15)	Networked Privileged Accesses				S				
SC-7(16)	Prevent Discovery of System Components				S				
SC-7(17)	Automated Enforcement of Protocol Formats				S				
SC-7(18)	Fail Secure				S				x
SC-7(19)	Block Communication from Non-Organizationally Configured Hosts				S				
SC-7(20)	Dynamic Isolation and Segregation				S				
SC-7(21)	Isolation of System Components				O/S				x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SC-7(22)	Separate Subnets for Connecting to Different Security Domains				S				
SC-7(23)	Disable Sender Feedback on Protocol Validation Failure				S				
SC-7(24)	Personally Identifiable Information	x			O/S	x			
SC-7(25)	Unclassified National Security Connections	x			O				
SC-7(26)	Classified National Security System Connections	x			O				
SC-7(27)	Unclassified Non-National Security System Connections	x			O				
SC-7(28)	Connections to Public Networks	x			O				
SC-7(29)	Separate Subnets to Isolate Functions	x			S				
SC-8	Transmission Confidentiality and Integrity				S			x	x
SC-8(1)	Cryptographic Protection				S			x	x
SC-8(2)	Pre- and Post-Transmission Handling				S				
SC-8(3)	Cryptographic Protection for Message Externals				S				
SC-8(4)	Conceal or Randomize Communications				S				
SC-8(5)	Protected Distribution System	x			S				
SC-10	Network Disconnect				S			x	x
SC-11	Trusted Path				S				
SC-11(1)	Irrefutable Communications Path				S				
SC-12	Cryptographic Key Establishment and Management				O/S		x	x	x
SC-12(1)	Availability				O/S				x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SC-12(2)	Symmetric Keys				O/S				
SC-12(3)	Asymmetric Keys				O/S				
SC-12(6)	Physical Control of Keys	x			O/S				
SC-13	Cryptographic Protection				S		x	x	x
SC-15	Collaborative Computing Devices and Applications				S		x	x	x
SC-15(1)	Physical or Logical Disconnect				S				
SC-15(3)	Disabling and Removal in Secure Work Areas				O				
SC-15(4)	Explicitly Indicate Current Participants				S				
SC-16	Transmission of Security and Privacy Attributes				S				
SC-16(1)	Integrity Verification				S				
SC-16(2)	Anti-Spoofing Mechanisms	x			S				
SC-16(3)	Cryptographic Binding	x			S				
SC-17	Public Key Infrastructure Certificates				O/S			x	x
SC-18	Mobile Code				O			x	x
SC-18(1)	Identify Unacceptable Code and Take Corrective Actions				S				
SC-18(2)	Acquisition, Development, and Use				O				
SC-18(3)	Prevent Downloading and Execution				S				
SC-18(4)	Prevent Automatic Execution				S				
SC-18(5)	Allow Execution Only in Confined Environments				S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SC-19	Voice over Internet Protocol			x					
SC-20	Secure Name/Address Resolution Service (Authoritative Source)				S		x	x	x
SC-20(2)	Data Origin and Integrity				S				
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)				S		x	x	x
SC-22	Architecture and Provisioning for Name/Address Resolution Service				S		x	x	x
SC-23	Session Authenticity				S			x	x
SC-23(1)	Invalidate Session Identifiers at Logout				S				
SC-23(3)	Unique System-Generated Session Identifiers				S				
SC-23(5)	Allowed Certificate Authorities				S				
SC-24	Fail in Known State				S				x
SC-25	Thin Nodes				S				
SC-26	Decoys				S				
SC-27	Platform-Independent Applications				S				
SC-28	Protection of Information at Rest				S			x	x
SC-28(1)	Cryptographic Protection		x		S			x	x
SC-28(2)	Offline Storage				O				
SC-28(3)	Cryptographic Keys	x			O/S				
SC-29	Heterogeneity				O				
SC-29(1)	Virtualization Techniques				O				
SC-30	Concealment and Misdirection				O				
SC-30(2)	Randomness				O				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SC-30(3)	Change Processing and Storage Locations				O				
SC-30(4)	Misleading Information				O				
SC-30(5)	Concealment of System Components				O				
SC-31	Covert Channel Analysis				O				
SC-31(1)	Test Covert Channels for Exploitability				O				
SC-31(2)	Maximum Bandwidth				O				
SC-31(3)	Measure Bandwidth in Operational Environments				O				
SC-32	System Partitioning				O/S				
SC-32(1)	Separate Physical Domains for Privileged Functions	x			O/S				
SC-34	Non-Modifiable Executable Programs				S				
SC-34(1)	No Writable Storage				O				
SC-34(2)	Integrity Protection and Read-Only Media				O				
SC-34(3)	Hardware-Based Protection			→ SC-51					
SC-35	External Malicious Code Identification				S				
SC-36	Distributed Processing and Storage				O				
SC-36(1)	Polling Techniques				O				
SC-36(2)	Synchronization	x			O				
SC-37	Out-of-Band Channels				O				
SC-37(1)	Ensure Delivery and Transmission				O				
SC-38	Operations Security				O				
SC-39	Process Isolation				S		x	x	x

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SC-39(1)	Hardware Separation				S				
SC-39(2)	Separate Execution Domain per Thread				S				
SC-40	Wireless Link Protection				S				
SC-40(1)	Electromagnetic Interference				S				
SC-40(2)	Reduce Detection Potential				S				
SC-40(3)	Imitative or Manipulative Communications Deception				S				
SC-40(4)	Signal Parameter Identification				S				
SC-41	Port and I/O Device Access				O/S				
SC-42	Sensor Capability and Data		x		S				
SC-42(1)	Reporting to Authorized Individuals or Roles				O				
SC-42(2)	Authorized Use				O				
SC-42(3)	Prohibit Use of Devices			→ SC-42					
SC-42(4)	Notice of Collection	x			O				
SC-42(5)	Collection Minimization	x			O				
SC-43	Usage Restrictions				O/S				
SC-44	Detonation Chambers				S				
SC-45	System Time Synchronization	x			S				
SC-45(1)	Synchronization with Authoritative Time Source	x			S				
SC-45(2)	Secondary Authoritative Time Source	x			S				
SC-46	Cross Domain Policy Enforcement	x			S				
SC-47	Alternate Communications Paths	x			O/S				
SC-48	Sensor Relocation	x			O/S				

SYSTEM AND COMMUNICATIONS (SC)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SC-48(1)	Dynamic Relocation of Sensors or Monitoring Capabilities	x			O/S				
SC-49	Hardware-Enforced Separation and Policy Enforcement	x			O/S				
SC-50	Software-Enforced Separation and Policy Enforcement	x			O/S				
SC-51	Hardware-Based Protection	x			O/S				
SYSTEM AND INFORMATION INTEGRITY (SI)									
SI-1	Policy and Procedures				O	x	x	x	x
SI-2	Flaw Remediation				O		x	x	x
SI-2(1)	Central Management			→ PL-9					
SI-2(2)	Automated Flaw Remediation Status				O			x	x
SI-2(3)	Time to Remediate Flaws and Benchmarks for Corrective Actions				O				
SI-2(4)	Automated Patch Management Tools	x			O/S				
SI-2(5)	Automatic Software and Firmware Updates				O/S				
SI-2(6)	Removal of Previous Versions of Software and Firmware				O/S				
SI-3	Malicious Code Protection		x		O/S		x	x	x
SI-3(1)	Central Management			→ PL-9					
SI-3(2)	Automatic Updates			→ SI-3					
SI-3(4)	Updates Only by Privileged Users				O/S				
SI-3(6)	Testing and Verification				O				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SI-3(7)	Nonsignature-Based Detection			→ SI-3					
SI-3(8)	Detect Unauthorized Commands				S				
SI-3(9)	Authenticate Remote Commands			→ AC-17(10)					
SI-3(10)	Malicious Code Analysis				O				
SI-4	System Monitoring				O/S		x	x	x
SI-4(1)	System-Wide Intrusion Detection System				O/S				
SI-4(2)	Automated Tools and Mechanisms for Real-Time Analysis				S			x	x
SI-4(3)	Automated Tool and Mechanism Integration				S				
SI-4(4)	Inbound and Outbound Communications Traffic				S			x	x
SI-4(5)	System-Generated Alerts				S			x	x
SI-4(7)	Automated Response to Suspicious Events				S				
SI-4(9)	Testing of Monitoring Tools and Mechanisms				O				
SI-4(10)	Visibility of Encrypted Communications				O				x
SI-4(11)	Analyze Communications Traffic Anomalies				O/S				
SI-4(12)	Automated Organization-Generated Alerts				O/S				x
SI-4(13)	Analyze Traffic and Event Patterns				O/S				
SI-4(14)	Wireless Intrusion Detection				S				x
SI-4(15)	Wireless to Wireline Communications				S				
SI-4(16)	Correlate Monitoring Information				O/S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SI-4(17)	Integrated Situational Awareness				O				
SI-4(18)	Analyze Traffic and Covert Exfiltration				O/S				
SI-4(19)	Risk for Individuals				O				
SI-4(20)	Privileged Users				S				x
SI-4(21)	Probationary Periods				O				
SI-4(22)	Unauthorized Network Services				S				x
SI-4(23)	Host-Based Devices				O				
SI-4(24)	Indicators of Compromise				S				
SI-4(25)	Optimize Network Traffic Analysis	x			S				
SI-5	Security Alerts, Advisories, and Directives				O		x	x	x
SI-5(1)	Automated Alerts and Advisories				O				x
SI-6	Security and Privacy Function Verification				S				x
SI-6(2)	Automation Support for Distributed Testing				S				
SI-6(3)	Report Verification Results				O				
SI-7	Software, Firmware, and Information Integrity				O/S			x	x
SI-7(1)	Integrity Checks				S			x	x
SI-7(2)	Automated Notifications of Integrity Violations				S				x
SI-7(3)	Centrally Managed Integrity Tools				O				
SI-7(5)	Automated Response to Integrity Violations				S				x
SI-7(6)	Cryptographic Protection				S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SI-7(7)	Integration of Detection and Response				O			x	x
SI-7(8)	Auditing Capability for Significant Events				S				
SI-7(9)	Verify Boot Process				S				
SI-7(10)	Protection of Boot Firmware				S				
SI-7(11)	Confined Environments with Limited Privileges			→ CM-7(6)					
SI-7(12)	Integrity Verification				O/S				
SI-7(13)	Code Execution in Protected Environments			→ CM-7(7)					
SI-7(14)	Binary or Machine Executable Code			→ CM-7(8)					
SI-7(15)	Code Authentication				S				x
SI-7(16)	Time Limit on Process Execution without Supervision				O				
SI-7(17)	Runtime Application Self-Protection	x			O/S				
SI-8	Spam Protection				O			x	x
SI-8(1)	Central Management			→ PL-9					
SI-8(2)	Automatic Updates				S			x	x
SI-8(3)	Continuous Learning Capability				S				
SI-10	Information Input Validation				S			x	x
SI-10(1)	Manual Override Capability				O/S				
SI-10(2)	Review and Resolve Errors				O				
SI-10(3)	Predictable Behavior				O/S				
SI-10(4)	Timing Interactions				S				
SI-10(5)	Restrict Inputs to Trusted Sources and Approved Formats				S				
SI-10(6)	Injection Prevention	x			S				

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SI-11	Error Handling				S			x	x
SI-12	Information Management and Retention				O	x	x	x	x
SI-12(1)	Limit Personally Identifiable Information Elements	x			O	x			
SI-12(2)	Minimize Personally Identifiable Information in Testing, Training, and Research	x			O	x			
SI-12(3)	Information Disposal	x			O	x			
SI-13	Predictable Failure Prevention				O				
SI-13(1)	Transferring Component Responsibilities				O				
SI-13(3)	Manual Transfer Between Components				O				
SI-13(4)	Standby Component Installation and Notification				O/S				
SI-13(5)	Failover Capability				O				
SI-14	Non-Persistence				O				
SI-14(1)	Refresh from Trusted Sources				O				
SI-14(2)	Non-Persistent Information	x			O				
SI-14(3)	Non-Persistent Connectivity	x			O				
SI-15	Information Output Filtering				S				
SI-16	Memory Protection				S			x	x
SI-17	Fail-Safe Procedures				S				
SI-18	Personally Identifiable Information Quality Operations	x			O/S	x			
SI-18(1)	Automation Support	x			O/S				
SI-18(2)	Data Tags	x			O/S				
SI-18(3)	Collection	x			O/S				

SYSTEM AND INFORMATION INTEGRITY (SI)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SI-18(4)	Individual Requests	x			O/S	x			
SI-18(5)	Notice of Correction or Deletion	x			O/S				
SI-19	De-Identification	x			O/S	x			
SI-19(1)	Collection	x			O/S				
SI-19(2)	Archiving	x			O/S				
SI-19(3)	Release	x			O/S				
SI-19(4)	Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers	x			S				
SI-19(5)	Statistical Disclosure Control	x			O/S				
SI-19(6)	Differential Privacy	x			O/S				
SI-19(7)	Validated Algorithms Software	x			O				
SI-19(8)	Motivated Intruder	x			O/S				
SI-20	Tainting	x			O/S				
SI-21	Information Refresh	x			O/S				
SI-22	Information Diversity	x			O/S				
SI-23	Information Fragmentation	x			O/S				

SUPPLY CHAIN RISK MANAGEMENT (SR)

SR-1	Policy and Procedures	x			O		x	x	x
SR-2	Supply Chain Risk Management Plan	x			O		x	x	x
SR-2(1)	Establish SCRM Team	x			O		x	x	x
SR-3	Supply Chain Controls and Processes	x			O/S		x	x	x
SR-3(1)	Diverse Supply Base	x			O				
SR-3(2)	Limitation of Harm	x			O				

SUPPLY CHAIN RISK MANAGEMENT (SR)

Control Number	Control Name (Control Enhancement Name)	New	Revised	Withdrawn	Implemented By	Privacy Control Baseline	Control Baseline Low	Control Baseline Moderate	Control Baseline High
SR-3(3)	Sub-Tier Flow Down	x			O				
SR-4	Provenance	x			O				
SR-4(1)	Identity	x			O				
SR-4(2)	Track and Trace	x			O				
SR-4(3)	Validate as Genuine and Not Altered	x			O				
SR-4(4)	Supply Chain Integrity — Pedigree	x			O				
SR-5	Acquisition Strategies, Tools, and Methods	x			O		x	x	x
SR-5(1)	Adequate Supply	x			O				
SR-5(2)	Assessments Prior to Selection, Acceptance, Modification, or Update	x			O				
SR-6	Supplier Assessments and Reviews	x			O			x	x
SR-6(1)	Testing and Analysis	x			O				
SR-7	Supply Chain Operations Security	x			O				
SR-8	Notification Agreements	x			O		x	x	x
SR-9	Tamper Resistance and Detection	x			O				x
SR-9(1)	Multiple Stages of System Development Life Cycle	x			O				x
SR-10	Inspection of Systems or Components	x			O		x	x	x
SR-11	Component Authenticity	x			O		x	x	x
SR-11(1)	Anti-Counterfeit Training	x			O		x	x	x
SR-11(2)	Configuration Control for Component Service and Repair	x			O		x	x	x
SR-11(3)	Anti-Counterfeit Scanning	x			O				
SR-12	Component Disposal	x			O		x	x	x

Legend for NIST 800-53 Rev 5.0, Security Control Guide

Implemented By (sixth column)

- S: A control or control enhancement that is typically implemented by an organizational system through technical means.
- O: A control or control enhancement that is typically implemented by an organization (i.e., by a human through nontechnical means).
- O/S: A control or control enhancement that can be implemented by an organization or a system or a combination of the two.

Control Baseline Allocation (eighth–tenth columns)

- A control or control enhancement that has been allocated to a control baseline is indicated by an "X" in the column for that baseline.
- A control or control enhancement that has not been allocated to a control baseline is indicated by a blank cell. Controls and control enhancements that are not allocated to any baseline can be selected on an optional basis.

COMPLIANCE THROUGH RISK MANAGEMENT

TALATEK LLC
COMPLIANCE THROUGH RISK MANAGEMENT

Registered Provider Organization

FedRAMP

CERBERUS SENTINEL