13.1.[Access Control] (AC)

AC-1[Access Control Policy and Procedures]The organization:

AC-2[Account Management]The organization:

AC-3[Access Enforcement]The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC-4[Information Flow Enforcement]The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on

AC-5[Separation of Duties]The organization:

AC-6[Least Privilege]The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

AC-7[Unsuccessful Logon Attempts]The information system:

AC-8[System Use Notification]The information system:

AC-9[Previous Logon (access) Notification]The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

AC-10[Concurrent Session Control]The information system limits the number of concurrent sessions for each

AC-11[Session Lock]The information system:

AC-12[Session Termination]The information system automatically terminates a user session after

AC-13[Supervision and Review - Access Control]

AC-14[Permitted Actions Without Identification or Authentication]The organization:

AC-15[Automated Marking]

AC-16[Security Attributes]The organization:

AC-17[Remote Access]The organization:

AC-18[Wireless Access]The organization:

AC-19[Access Control for Mobile Devices]The organization:

AC-20[Use of External Information Systems]The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

AC-21[Information Sharing]The organization:

AC-22[Publicly Accessible Content]The organization:

AC-23[Data Mining Protection]The organization employs

AC-24[Access Control Decisions]The organization establishes procedures to ensure

AC-25[Reference Monitor]The information system implements a reference monitor for

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.2.[Awareness and Training] (AT)

AT-1[Security Awareness and Training Policy and Procedures]The organization:

AT-2[Security Awareness Training]The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

AT-3[Role-based Security Training]The organization provides role-based security training to personnel with assigned security roles and responsibilities:

AT-4[Security Training Records]The organization:

AT-5[Contacts with Security Groups and Associations]

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.3.[Audit and Accountability] (AU)

AU-1[Audit and Accountability Policy and Procedures]The organization:

AU-2[Audit Events]The organization:

AU-3[Content of Audit Records]The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

AU-4[Audit Storage Capacity]The organization allocates audit record storage capacity in accordance with

AU-5[Response to Audit Processing Failures]The information system:

AU-6[Audit Review, Analysis, and Reporting]The organization:

AU-7[Audit Reduction and Report Generation]The information system provides an audit reduction and report generation capability that:

AU-8[Time Stamps]The information system:

AU-9[Protection of Audit Information]The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

AU-10[Non-repudiation]The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed

AU-11[Audit Record Retention]The organization retains audit records for

AU-12[Audit Generation]The information system:

AU-13[Monitoring for Information Disclosure]The organization monitors

AU-14[Session Audit]The information system provides the capability for authorized users to select a user session to capture/record or view/hear.

AU-15[Alternate Audit Capability]The organization provides an alternate audit capability in the event of a failure in primary audit capability that provides

AU-16[Cross-organizational Auditing]The organization employs

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.4.[Security Assessment and Authorization] (CA)

CA-1[Security Assessment and Authorization Policy and Procedures]The organization:

CA-2[Security Assessments]The organization:

CA-3[System Interconnections]The organization:

CA-4[Security Certification]

CA-5[Plan of Action and Milestones]The organization:

CA-6[Security Authorization]The organization:

CA-7[Continuous Monitoring]The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

CA-8[Penetration Testing]The organization conducts penetration testing

CA-9[Internal System Connections]The organization:

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.5.[Configuration Management] (CM)

CM-1[Configuration Management Policy and Procedures]The organization:

CM-2[Baseline Configuration]The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

CM-3[Configuration Change Control]The organization:

CM-4[Security Impact Analysis]The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

CM-5[Access Restrictions for Change]The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

CM-6[Configuration Settings]The organization:

CM-7[Least Functionality]The organization:

CM-8[Information System Component Inventory]The organization:

CM-9[Configuration Management Plan]The organization develops, documents, and implements a configuration management plan for the information system that:

CM-10[Software Usage Restrictions]The organization:

CM-11[User-installed Software]The organization:

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.6.[Contingency Planning] (CP)

CP-1[Contingency Planning Policy and Procedures]The organization:

CP-2[Contingency Plan]The organization:

CP-3[Contingency Training]The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

CP-4[Contingency Plan Testing]The organization:

CP-5[Contingency Plan Update]

CP-6[Alternate Storage Site]The organization:

CP-7[Alternate Processing Site]The organization:

CP-8[Telecommunications Services]The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of

CP-9[Information System Backup]The organization:

CP-10[Information System Recovery and Reconstitution]The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

CP-11[Alternate Communications Protocols]The information system provides the capability to employ

CP-12[Safe Mode]The information system, when

CP-13[Alternative Security Mechanisms]The organization employs

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.7.[Identification and Authentication] (IA)

IA-1[Identification and Authentication Policy and Procedures]The organization:

IA-2[Identification and Authentication (organizational Users)]The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

IA-3[Device Identification and Authentication]The information system uniquely identifies and authenticates

IA-4[Identifier Management]The organization manages information system identifiers by:

IA-5[Authenticator Management]The organization manages information system authenticators by:

IA-6[Authenticator Feedback]The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

IA-7[Cryptographic Module Authentication]The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

IA-8[Identification and Authentication (non-organizational Users)]The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

IA-9[Service Identification and Authentication]The organization identifies and authenticates

IA-10[Adaptive Identification and Authentication]The organization requires that individuals accessing the information system employ

IA-11[Re-authentication]The organization requires users and devices to re-authenticate when

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.8.[Incident Response] (IR)

IR-1[Incident Response Policy and Procedures]The organization:

IR-2[Incident Response Training]The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

IR-3[Incident Response Testing]The organization tests the incident response capability for the information system

IR-4[Incident Handling]The organization:

IR-5[Incident Monitoring]The organization tracks and documents information system security incidents.

IR-6[Incident Reporting]The organization:

IR-7[Incident Response Assistance]The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

IR-8[Incident Response Plan]The organization:

IR-9[Information Spillage Response]The organization responds to information spills by:

IR-10[Integrated Information Security Analysis Team]The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.9.[Maintenance] (MA)

MA-1[System Maintenance Policy and Procedures]The organization:

MA-2[Controlled Maintenance]The organization:

MA-3[Maintenance Tools]The organization approves, controls, and monitors information system maintenance tools.

MA-4[Nonlocal Maintenance]The organization:

MA-5[Maintenance Personnel]The organization:

MA-6[Timely Maintenance]The organization obtains maintenance support and/or spare parts for

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.10.[Media Protection] (MP)

MP-1[Media Protection Policy and Procedures]The organization:

MP-2[Media Access]The organization restricts access to

MP-3[Media Marking]The organization:

MP-4[Media Storage]The organization:

MP-5[Media Transport]The organization:

MP-6[Media Sanitization]The organization:

MP-7[Media Use]The organization

MP-8[Media Downgrading]The organization:

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.11.[Physical and Environmental Protection] (PE)

PE-1[Physical and Environmental Protection Policy and Procedures]The organization:

PE-2[Physical Access Authorizations]The organization:

PE-3[Physical Access Control]The organization:

PE-4[Access Control for Transmission Medium]The organization controls physical access to

PE-5[Access Control for Output Devices]The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

PE-6[Monitoring Physical Access]The organization:

PE-7[Visitor Control]

PE-8[Visitor Access Records]The organization:

PE-9[Power Equipment and Cabling]The organization protects power equipment and power cabling for the information system from damage and destruction.

PE-10[Emergency Shutoff]The organization:

PE-11[Emergency Power]The organization provides a short-term uninterruptible power supply to facilitate

PE-12[Emergency Lighting]The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

PE-13[Fire Protection]The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

PE-14[Temperature and Humidity Controls]The organization:

PE-15[Water Damage Protection]The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

PE-16[Delivery and Removal]The organization authorizes, monitors, and controls

PE-17[Alternate Work Site]The organization:

PE-18[Location of Information System Components]The organization positions information system components within the facility to minimize potential damage from

PE-19[Information Leakage]The organization protects the information system from information leakage due to electromagnetic signals emanations.

PE-20[Asset Monitoring and Tracking]The organization:

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.12.[Planning] (PL)

PL-1[Security Planning Policy and Procedures]The organization:

PL-2[System Security Plan]The organization:

PL-3[System Security Plan Update]

PL-4[Rules of Behavior]The organization:

PL-5[Privacy Impact Assessment]

PL-6[Security-related Activity Planning]

PL-7[Security Concept of Operations]The organization:

PL-8[Information Security Architecture]The organization:

PL-9[Central Management]The organization centrally manages

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.13.[Personnel Security] (PS)

PS-1[Personnel Security Policy and Procedures]The organization:

PS-2[Position Risk Designation]The organization:

PS-3[Personnel Screening]The organization:

PS-4[Personnel Termination]The organization, upon termination of individual employment:

PS-5[Personnel Transfer]The organization:

PS-6[Access Agreements]The organization:

PS-7[Third-party Personnel Security]The organization:

PS-8[Personnel Sanctions]The organization:

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.14.[Risk Assessment] (RA)

RA-1[Risk Assessment Policy and Procedures]The organization:

RA-2[Security Categorization]The organization:

RA-3[Risk Assessment]The organization:

RA-4[Risk Assessment Update]

RA-5[Vulnerability Scanning]The organization:

RA-6[Technical Surveillance Countermeasures Survey]The organization employs a technical surveillance countermeasures survey at

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.15.[System and Services Acquisition] (SA)

SA-1[System and Services Acquisition Policy and Procedures]The organization:

SA-2[Allocation of Resources]The organization:

SA-3[System Development Life Cycle]The organization:

SA-4[Acquisition Process]The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

SA-5[Information System Documentation]The organization:

SA-6[Software Usage Restrictions]

SA-7[User-installed Software]

SA-8[Security Engineering Principles]The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

SA-9[External Information System Services]The organization:

SA-10[Developer Configuration Management]The organization requires the developer of the information system, system component, or information system service to:

SA-11[Developer Security Testing and Evaluation]The organization requires the developer of the information system, system component, or information system service to:

SA-12[Supply Chain Protection]The organization protects against supply chain threats to the information system, system component, or information system service by employing

SA-13[Trustworthiness]The organization:

SA-14[Criticality Analysis]The organization identifies critical information system components and functions by performing a criticality analysis for

SA-15[Development Process, Standards, and Tools]The organization:

SA-16[Developer-provided Training]The organization requires the developer of the information system, system component, or information system service to provide

SA-17[Developer Security Architecture and Design]The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

SA-18[Tamper Resistance and Detection]The organization implements a tamper protection program for the information system, system component, or information system service.

SA-19[Component Authenticity]The organization:

SA-20[Customized Development of Critical Components]The organization re-implements or custom develops

SA-21[Developer Screening]The organization requires that the developer of

SA-22[Unsupported System Components]The organization:

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.16.[System and Communications Protection] (SC)

SC-1[System and Communications Protection Policy and Procedures]The organization:

SC-2[Application Partitioning]The information system separates user functionality (including user interface services) from information system management functionality.

SC-3[Security Function Isolation]The information system isolates security functions from nonsecurity functions.

SC-4[Information in Shared Resources]The information system prevents unauthorized and unintended information transfer via shared system resources.

SC-5[Denial of Service Protection]The information system protects against or limits the effects of the following types of denial of service attacks:

SC-6[Resource Availability]The information system protects the availability of resources by allocating

SC-7[Boundary Protection]The information system:

SC-8[Transmission Confidentiality and Integrity]The information system protects the

SC-9[Transmission Confidentiality]

SC-10[Network Disconnect]The information system terminates the network connection associated with a communications session at the end of the session or after

SC-11[Trusted Path]The information system establishes a trusted communications path between the user and the following security functions of the system:

SC-12[Cryptographic Key Establishment and Management]The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with

SC-13[Cryptographic Protection]The information system implements

SC-14[Public Access Protections]

SC-15[Collaborative Computing Devices]The information system:

SC-16[Transmission of Security Attributes]The information system associates

SC-17[Public Key Infrastructure Certificates]The organization issues public key certificates under an

SC-18[Mobile Code]The organization:

SC-19[Voice Over Internet Protocol]The organization:

SC-20[Secure Name / Address Resolution Service (authoritative Source)]The information system:

SC-21[Secure Name / Address Resolution Service (recursive or Caching Resolver)]The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

SC-22[Architecture and Provisioning for Name / Address Resolution Service]The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

SC-23[Session Authenticity]The information system protects the authenticity of communications sessions.

SC-24[Fail in Known State]The information system fails to a

SC-25[Thin Nodes]The organization employs

SC-26[Honeypots]The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

SC-27[Platform-independent Applications]The information system includes:

SC-28[Protection of Information at Rest]The information system protects the

SC-29[Heterogeneity]The organization employs a diverse set of information technologies for

SC-30[Concealment and Misdirection]The organization employs

SC-31[Covert Channel Analysis]The organization:

SC-32[Information System Partitioning]The organization partitions the information system into

SC-33[Transmission Preparation Integrity]

SC-34[Non-modifiable Executable Programs]The information system at

SC-35[Honeyclients]The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.

SC-36[Distributed Processing and Storage]The organization distributes

SC-37[Out-of-band Channels]The organization employs

SC-38[Operations Security]The organization employs

SC-39[Process Isolation]The information system maintains a separate execution domain for each executing process.

SC-40[Wireless Link Protection]The information system protects external and internal

SC-41[Port and I/O Device Access]The organization physically disables or removes

SC-42[Sensor Capability and Data]The information system:

SC-43[Usage Restrictions]The organization:

SC-44[Detonation Chambers]The organization employs a detonation chamber capability within

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.17.[System and Information Integrity] (SI)

SI-1[System and Information Integrity Policy and Procedures]The organization:

SI-2[Flaw Remediation]The organization:

SI-3[Malicious Code Protection]The organization:

SI-4[Information System Monitoring]The organization:

SI-5[Security Alerts, Advisories, and Directives]The organization:

SI-6[Security Function Verification]The information system:

SI-7[Software, Firmware, and Information Integrity]The organization employs integrity verification tools to detect unauthorized changes to

SI-8[Spam Protection]The organization:

SI-9[Information Input Restrictions]

SI-10[Information Input Validation]The information system checks the validity of

SI-11[Error Handling]The information system:

SI-12[Information Handling and Retention]The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

SI-13[Predictable Failure Prevention]The organization:

SI-14[Non-persistence]The organization implements non-persistent

SI-15[Information Output Filtering]The information system validates information output from

SI-16[Memory Protection]The information system implements

SI-17[Fail-safe Procedures]The information system implements

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

13.18.[Program Management] (PM)

PM-1[Information Security Program Plan]The organization:

PM-2[Senior Information Security Officer]The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

PM-3[Information Security Resources]The organization:

PM-4[Plan of Action and Milestones Process]The organization:

PM-5[Information System Inventory]The organization develops and maintains an inventory of its information systems.

PM-6[Information Security Measures of Performance]The organization develops, monitors, and reports on the results of information security measures of performance.

PM-7[Enterprise Architecture]The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

PM-8[Critical Infrastructure Plan]The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

PM-9[Risk Management Strategy]The organization:

PM-10[Security Authorization Process]The organization:

PM-11[Mission/business Process Definition]The organization:

PM-12[Insider Threat Program]The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

PM-13[Information Security Workforce]The organization establishes an information security workforce development and improvement program.

PM-14[Testing, Training, and Monitoring]The organization:

PM-15[Contacts with Security Groups and Associations]The organization establishes and institutionalizes contact with selected groups and associations within the security community:

PM-16[Threat Awareness Program]The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |

|  |  |  |
| --- | --- | --- |
| col one, row one | col two, row one | col three, row one |