Table 1

Control Topic	Mapped NIST SP 800-53 Control ID	Control Title	Control Family
Least Privilege	AC-6	Least Privilege	Access Control (AC)
	AC-6(1)	Authorize Access to Security Functions	Access Control (AC)
	AC-6(2)	Non-privileged Access for Nonsecurity Functions	Access Control (AC)
	AC-6(5)	Privileged Accounts	Access Control (AC)
	AC-6(7)	Review of User Privileges	Access Control (AC)
	SA-8(14)	Least Privilege — Secure Engineering	System and Services Acquisition (SA)
Disaster Recovery Plans	CP-2	Contingency Plan	Contingency Planning (CP)
	CP-2(3)	Resume Mission and Business Functions	Contingency Planning (CP)
	CP-2(4)	Resume All Mission and Business Functions	Contingency Planning (CP)
	CP-4	Contingency Plan Testing	Contingency Planning (CP)
	CP-6	Alternate Storage Site	Contingency Planning (CP)
	CP-7	Alternate Processing Site	Contingency Planning (CP)
	CP-9	System Backup	Contingency Planning (CP)
	CP-10	System Recovery and Reconstitution	Contingency Planning (CP)
Password Policies	IA-5	Authenticator Management	Identification and Authentication (IA)
	IA-5(1)	Password-based Authentication	Identification and Authentication (IA)

	IA-5(4)	Automated Support for Password Strength	Identification and Authentication (IA)
	IA-5(6)	Protection of Authenticators	Identification and Authentication (IA)
	IA-5(18)	Password Managers	Identification and Authentication (IA)
Access Control Policies	AC-1	Policy and Procedures	Access Control (AC)
	AC-3	Access Enforcement	Access Control (AC)
	AC-17	Remote Access	Access Control (AC)
	AC-19	Access Control for Mobile Devices	Access Control (AC)
	PL-2	System Security and Privacy Plans	Planning (PL)
Account Management Policies	AC-2	Account Management	Access Control (AC)
	AC-2(1)	Automated System Account Management	Access Control (AC)
	AC-2(4)	Automated Audit Actions	Access Control (AC)
	AC-2(5)	Inactivity Logout	Access Control (AC)

	AC-2(7)	Privileged User Accounts	Access Control (AC)
	AC-2(9)	Restrictions on use of Shared and Group Accounts	Access Control (AC)
	AC-2(13)	Disable Accounts for High-risk Individuals	Access Control (AC)
Separation of Duties	AC-5	Separation of Duties	Access Control (AC)
	AC-3(2)	Dual Authorization	Access Control (AC)
	PS-2	Position Risk Designation	Personnel Security (PS)
Firewall	SC-7	Boundary Protection	System and Communications Protection (SC)
IDS/IPS	SI-4	System Monitoring	System and Information Integrity (SI)
Encryption	SC-12	Cryptographic Key Establishment and Management	System and Communications Protection (SC)
	SC-13	Cryptographic Protection	System and Communications Protection (SC)
	SC-28	Protection of Information at Rest	System and Communications Protection (SC)
Backups	CP-9	System Backup	Contingency Planning (CP)
	CP-10	System Recovery and Reconstitution	Contingency Planning (CP)

Password management	IA-5	Authenticator Management	Identification and Authentication (IA)
Antivirus (AV) software	SI-3	Malicious Code Protection	System and Information Integrity (SI)
Manual monitoring, maintenance, and intervention	MA-2	Controlled Maintenance.	System and Information Integrity (SI)
	MA-6	Timely Maintenance	System and Information Integrity (SI)
	SI-4	System Monitoring	Maintenance (MA)
Time-controlled safe	PE-3	Physical Access Control	Physical and Environmental Protection
Adequate lighting	PE-12	Emergency Lighting	Physical and Environmental Protection
Closed-circuit television (CCTV)	PE-6	Monitoring Physical Access	Physical and Environmental Protection
Locking cabinets (for network gear)	PE-3(4)	Physical Access Control - Lockable Casings	Physical and Environmental Protection
Signage indicating alarm service provider	PE-6(3)	Monitoring Physical Access - Video Surveillance	Physical and Environmental Protection

Locks	PE-3	Physical Access Control	Physical and Environmental Protection
Fire detection and prevention (fire alarm, sprinkler system, etc.)	PE-13	Fire Protection	Physical and Environmental Protection

Control Topic	Description	Related Controls
Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38.
	Authorize access for [Assignment: organization-defined individuals or roles] to: (a) [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; and (b) [Assignment: organization-defined security-relevant information].	AC-17, AC-18, AC-19, AU-9, PE-2.
	Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing nonsecurity functions.	AC-17, AC-18, AC-19, PL-4.
	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].	IA-2, MA-3, MA-4.
	(a) Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and (b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	CA-7.
	Implement the security design principle of least privilege in [Assignment: organization-defined systems or system components].	AC-6, CM-7.
Disaster Recovery Plans	Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, organizational risk tolerance, and system impact level.	CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12.
	Plan for the resumption of [Selection: all	
	[Withdrawn: Incorporated into CP-2(3).]	
	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests]. b. Review the contingency plan test results; and c. Initiate corrective actions, if needed.	AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2.
	Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.	CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.
	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and c. Provide controls at the alternate processing site that are equivalent to those at the primary site.	CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.
	a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protect the confidentiality, integrity, and availability of backup information.	CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.
	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.
Password Policies	Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk.	-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13.
	Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h).	IA-6.

	[Withdrawn: Incorporated into IA-5(1).]	
	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	RA-2.
	(a) Employ [Assignment: organization-defined password managers] to generate and manage passwords	
Access Control Policies	Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure.	IA-1, PM-9, PM-24, PS-8, SI-12.
	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8.
	Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.	AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4.
	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.	AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-2, IA-3, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SC-34, SC-43, SI-3, SI-4.
	System security and privacy plans are scoped to the system and system components within the defined authorization boundary and contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. The plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control. The control documentation describes how system-specific and hybrid controls are implemented and the plans and expectations regarding the functionality of the system. System security and privacy plans can also be used in the design and development of systems in support of life cycle-based security and privacy engineering processes. System security and privacy plans are living documents that are updated and adapted throughout the system development life cycle (e.g., during capability determination, analysis of alternatives, requests for proposal, and design reviews).	AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CM-13, CP-2, CP-4, IR-4, IR-8, MA-4, MA-5, MP-4, MP-5, PL-7, PL-8, PL-10, PL-11, PM-1, PM-7, PM-8, PM-9, PM-10, PM-11, RA-3, RA-8, RA-9, SA-5, SA-17, SA-22, SI-12, SR-2, SR-4.
Account Management Policies	Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.	AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37.
	Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage. Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.	
	Automatically audit account creation, modification, enabling, disabling, and removal actions.	AU-2, AU-6.
	Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out].	AC-11.

	Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. Privileged roles include key management, account management, database administration, system and network administration, and web administration. A role-based access scheme organizes permitted system access and privileges into roles. In contrast, an attribute-based access scheme specifies allowed system access and privileges based on attributes.	
	Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts.	
	Users who pose a significant security and/or privacy risk include individuals for whom reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes adverse impacts to organizational operations, organizational assets, individuals, other organizations, or the Nation. Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.	AU-6, SI-4.
Separation of Duties	Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and define system access authorizations to support separation of duties.	AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8, SA-17.
	Dual authorization, also known as two-person control, reduces risk related to insider threats. Dual authorization mechanisms require the approval of two authorized individuals to execute. To reduce the risk of collusion, organizations consider rotating dual authorization duties. Organizations consider the risk associated with implementing dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.	CP-9, MP-6.
	a. Assign a risk designation to all organizational positions; b. Establish screening criteria for individuals filling those positions; and c. Review and update position risk designations [Assignment: organization-defined frequency].	AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA-21, SI-12.
Firewall	Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.	AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PL-8, PM-12, SA-8, SA-17, SC-5, SC-26, SC-32, SC-35, SC-43.
IDS/IPS	System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.	AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10.
Encryption	Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and specify appropriate options, parameters, and levels. Organizations manage trust stores to ensure that only approved trust anchors are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems. NIST CMVP and NIST CAVP provide additional information on validated cryptographic modules and algorithms that can be used in cryptographic key management and establishment.	AC-17, AU-9, AU-10, CM-3, IA-3, IA-7, SA-4, SA-8, SA-9, SC-8, SC-11, SC-12, SC-13, SC-17, SC-20, SC-37, SC-40, SI-3, SI-7.
	Cryptography can be employed to support a variety of security solutions, including the protection of classified information and controlled unclassified information, the provision and implementation of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals. Cryptography can also be used to support random number and hash generation. Applicable standards include FIPS-validated and NSA-approved cryptography.	AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, AU-10, CM-11, CP-9, IA-3, IA-5, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-8, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SC-40, SI-3, SI-7.
	Information at rest refers to the state of information when it is not in process or in transit and is located on system components. These include internal/external drives, SANs, or databases. Protection focuses on confidentiality and integrity, using cryptographic mechanisms, file share scanning, and WORM technologies, or secure offline storage when necessary.	AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-12, SC-13, SC-34, SI-3, SI-7, SI-16.
Backups	a. Conduct backups of user-level, system-level, and documentation information on organization-defined components at defined frequencies aligned with recovery time and recovery point objectives; b. Protect the confidentiality, integrity, and availability of backup information.	CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.
	Provide for the recovery and reconstitution of the system to a known state within an organization-defined time period consistent with recovery time and recovery point objectives after a disruption, compromise, or failure.	CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.

Password management	Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Developers may deliver systems with default credentials, posing risks. Controls such as PL-4, PS-6, AC-3, AC-6, and SC-28 are applicable for protecting authenticators in possession of individuals or stored within systems.	AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13.
Antivirus (AV) software	System entry and exit points include firewalls, remote access servers, email/web servers, proxy servers, workstations, laptops, and mobile devices. Malicious code includes viruses, worms, spyware, and steganography. It can spread via email, web, or storage devices and exploit vulnerabilities. Various technologies can limit or eliminate its impact.	AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, PL-9, RA-5, SC-7, SC-23, SC-26, SC-28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15.
Manual monitoring, maintenance, and intervention	System maintenance applies to all maintenance by local or nonlocal entities, including scanners, copiers, and printers. Records should include date/time, maintenance details, personnel, escort, and equipment involved. Organizations consider supply chain risks for replacement components.	CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-4, SR-11.
	Organizations identify components that pose increased risk if unavailable and ensure support contracts are in place to maintain functionality.	CM-8, CP-2, CP-7, RA-7, SA-15, SI-13, SR-2, SR-3, SR-4.
	System monitoring includes external and internal activities, observing real-time audit logs or system behavior such as access patterns. Tools include intrusion detection, antivirus, scanning utilities, audit log monitors, and network analysis software.	AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10.
Time-controlled safe	Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas. Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.	AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.
Adequate lighting	The provision of emergency lighting applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Emergency lighting provisions for the system are described in the contingency plan for the organization. If emergency lighting for the system fails or cannot be provided, organizations consider alternate processing sites for power-related contingencies.	CP-2, CP-7.
Closed-circuit television (CCTV)	Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls, such as AU-2, if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.	AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.
Locking cabinets (for network gear)	The greatest risk from the use of portable devices—such as smart phones, tablets, and notebook computers—is theft. Organizations can employ lockable, physical casings to reduce or eliminate the risk of equipment theft. Such casings come in a variety of sizes, from units that protect a single notebook computer to full cabinets that can protect multiple servers, computers, and peripherals. Lockable physical casings can be used in conjunction with cable locks or lockdown plates to prevent the theft of the locked casing containing the computer equipment.	
Signage indicating alarm service provider	Video surveillance focuses on recording activity in specified areas for the purposes of subsequent review, if circumstances so warrant. Video recordings are typically reviewed to detect anomalous events or incidents. Monitoring the surveillance video is not required, although organizations may choose to do so. There may be legal considerations when performing and retaining video surveillance, especially if such surveillance is in a public location.	

Locks	Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas. Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers. Physical access control systems comply with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.	AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.
Fire detection and prevention (fire alarm, sprinkler system, etc.)	The provision of fire detection and suppression systems applies primarily to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate, or can be separated, from the energy sources providing power for the other parts of the facility.	AT-3.

Control Topic	References
Least Privilege	
Disaster Recovery Plans	
Password Policies	

	[FIPS 140-3], [FIPS 180-4], [FIPS 201-2], [FIPS 202], [IR 7539], [IR 7817], [IR 7849], [IR 7870], [IR 8040], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4]
	[IR 7874], [OMB A-130], [SP 800-100], [SP 800-12], [SP 800-30], [SP 800-39]
Access Control Policies	
Account Management Policies	

	[SP 800-162], [SP 800-178], [SP 800-192]
Separation of Duties	
	[5 CFR 731], [SP 800-181]
Firewall	
IDS/IPS	
Encryption	
Backups	

Password management	
Antivirus (AV) software	
Manual monitoring, maintenance, and intervention	
Time-controlled safe	
Adequate lighting	
Closed-circuit television (CCTV)	
Locking cabinets (for network gear)	
Signage indicating alarm service provider	

Locks	
Fire detection and prevention (fire alarm, sprinkler system, etc.)	