Table 1

Security hardening task	Description	Common uses
Baseline configurations	A documented set of specifications within a system that is used as a basis for future builds, releases, and updates.	To restore a system to a previous baseline after a network outage, or unauthorized changes on a baseline.

Security hardening task	Description	Common uses
Configuration checks	Updating the encryption standards for data that is stored in databases.	To see if there are any unauthorized changes to the system.

Security hardening task	Description	Common uses
Disabling unused ports	Ports can be blocked on firewalls, routers, servers, and more to prevent potentially dangerous network traffic from passing through.	Before an incident occurs, to prevent malicious actors from entering the network through the open port. Can be used after an incident to prevent future attacks from happening through unused open ports.

Security hardening task	Description	Common uses
Encryption using the latest standards	Rules or methods used to conceal outgoing data and uncover or decrypt the incoming data.	Can be implemented regularly to assess if the current encryption standards are secure and effective for your organization. The encryption standards can also be updated after a data breach.

Security hardening task	Description	Common uses
Firewall maintenance	Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.	This can happen regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks.

Security hardening task	Description	Common uses
Hardware & software disposal	Ensures that all old hardware is properly wiped of all data and disposed of.	Prevent the network from various threats by removing outdated or unused software or hardware that do not have the latest security patches or updates. Unpatched devices can allow malicious actors to easily access the network.

Security hardening task	Description	Common uses
Multifactor authentication (MFA)	A security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more.	Can help protect against brute force attacks and similar security events. MFA can be implemented at any time, and is mostly a technique that is set up once then maintained.

Security hardening task	Description	Common uses
Network access privileges	Network access privileges involves permitting, limiting, and/or blocking access privileges to network assets for people, roles, groups, IP addresses, MAC addresses, etc.	Reduces the risk of unauthorized users and outside traffic from accessing the internal network. This can be implemented once, or revisited depending on the likelihood of social engineering or brute force attacks.

Security hardening task	Description	Common uses
Network log analysis	The process of examining network logs to identify events of interest.	Can be configured to alert the security team when there is abnormal traffic on the network. This can be used either before an incident occurs, during to track network traffic, and can be configured in the response of a cybersecurity attack. A common tool used for analyzing network logs is a SIEM.
Password policies	The National Institute of Standards and Technology's (NIST) latest recommendations for password policies focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords.	Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack).

Security hardening task	Description	Common uses
Patch updates	A software and operating system (OS) update that addresses security vulnerabilities within a program or product.	Patch updates often contain fixes to security problems. It is important to keep systems up to date with the latest security patches because attackers will be alerted to the security vulnerability when patches are released. They will be more likely to target that vulnerability before people eventually apply the patches.
Penetration test (pen test)	A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes.	Pen tests are used to protect and prevent against potential attacks.

Security hardening task	Description	Common uses
Port filtering	A firewall function that blocks or allows certain port numbers to limit unwanted communication.	Port filtering is used to control network traffic and can prevent potential attackers from entering a private network.
Removing or disabling unused applications and services	Unused applications and services can become a point of vulnerability because they are less likely to be maintained or updated with new security features.	This procedure is used to reduce potential vulnerabilities within a network.

Security hardening task	Description	Common uses
Server and data storage backups	Server and data storage backups help protect data assets from being lost. Backups can be recorded and stored in a physical location or uploaded/synced to a cloud repository.	Backups are used to restore lost data from attacks, human error, equipment failures, and other unplanned losses.

Security hardening task	**CIS v8:** This framework is laser-focused on practical, technical security controls for hardening systems and networks.
Baseline configurations	**Control 4.1:** Establish and maintain a documented secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard; **Control 4.2:** Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard; **Control 4.6:** Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential;

Security hardening task	**CIS v8:** This framework is laser-focused on practical, technical security controls for hardening systems and networks.
Configuration checks	**Control 4.3:** Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes; **Control 7.5:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans; **Control 7.6:** Perform automated vulnerability scans of externally-exposed enterprise assets. Perform scans on a monthly, or more frequent, basis.

Security hardening task	CIS v8: This framework is laser-focused on practical, technical security controls for hardening systems and networks.
Disabling unused ports	**Control 4.8:** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function; **Control 13.9:** Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

Security hardening task	**CIS v8:** This framework is laser-focused on practical, technical security controls for hardening systems and networks.
Encryption using the latest standards	**Control 3.6:** Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt; **Control 3.9:** Encrypt data on removable media; Control 3.10: Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH); **Control 3.11:** Encrypt sensitive data at rest on servers, applications, and databases. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

Security hardening task	CIS v8: This framework is laser-focused on practical, technical security controls for hardening systems and networks.
Firewall maintenance	**Control 4.4:** Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent; **Control 4.4:** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed; **Control 13.4:** Perform traffic filtering between network segments, where appropriate.

Security hardening task	CIS v8: This framework is laser-focused on practical, technical security controls for hardening systems and networks.
Hardware & software disposal	**Control 3.5:** Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

Security hardening task	**CIS v8:** This framework is laser-focused on practical, technical security controls for hardening systems and networks.
Multifactor authentication (MFA)	**Control 6.3:** Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard; **Control 6.4:** Require MFA for remote network access; **Control 6.5:** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.

Security hardening task	**CIS v8:** This framework is laser-focused on practical, technical security controls for hardening systems and networks.
Network access privileges	**Control 6.1:** Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user; **Control 6.2:** Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. **Control 6.7:** Centralize access control for all enterprise assets through a directory service or SSO provider, where supported; **Control 6.8:** Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

Security hardening task	CIS v8: This framework is laser-focused on practical, technical security controls for hardening systems and networks.
Network log analysis	**Control 8.2:** Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets; **Control 8.2:** Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.
Password policies	**Control 5.2:** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.

Security hardening task	**CIS v8:** This framework is laser-focused on practical, technical security controls for hardening systems and networks.
Patch updates	**Control 7.3:** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis; **Control 7.4:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis; **Control 7.7:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
Penetration test (pen test)	**Control 18.1:** Establish and maintain a penetration testing program appropriate to the size, complexity, industry, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements; **Control 18.1:** Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

Security hardening task	CIS v8: This framework is laser-focused on practical, technical security controls for hardening systems and networks.
Port filtering	**Control 13.4:** Perform traffic filtering between network segments, where appropriate; **Control 13.4:** Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.
Removing or disabling unused applications and services	**Control 4.8:** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

Security hardening task	**CIS v8:** This framework is laser-focused on practical, technical security controls for hardening systems and networks.
Server and data storage backups	**Control 11.1:** Establish and maintain a documented data recovery process that includes detailed backup procedures. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard; **Control 11.1:** Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

Security hardening task	**NIST Cybersecurity Framework (CSF 2.0):** NIST CSF is risk-based and widely adopted in both public and private sectors.
Baseline configurations	**Platform Security (PR.PS):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability **o PR.PS-01:** Configuration management practices are established and applied

Security hardening task	**NIST Cybersecurity Framework (CSF 2.0):** NIST CSF is risk-based and widely adopted in both public and private sectors.
Configuration checks	**Platform Security (PR.PS):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability; **o PR.PS-04:** Log records are generated and made available for continuous monitoring

Security hardening task	NIST Cybersecurity Framework (CSF 2.0): NIST CSF is risk-based and widely adopted in both public and private sectors.
Disabling unused ports	**Technology Infrastructure Resilience (PR.IR):** Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience **o PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage

Security hardening task	**NIST Cybersecurity Framework (CSF 2.0):** NIST CSF is risk-based and widely adopted in both public and private sectors.
Encryption using the latest standards	**Data Security (PR.DS):** Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information **o PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected **o PR.DS-10:** The confidentiality, integrity, and availability of data-in-use are protected

Security hardening task	NIST Cybersecurity Framework (CSF 2.0): NIST CSF is risk-based and widely adopted in both public and private sectors.
Firewall maintenance	**Technology Infrastructure Resilience (PR.IR):** Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience **o PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage; **Continuous Monitoring (DE.CM):** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events **o DE.CM-01:** Networks and network services are monitored to find potentially adverse events

Security hardening task	NIST Cybersecurity Framework (CSF 2.0): NIST CSF is risk-based and widely adopted in both public and private sectors.
Hardware & software disposal	**Asset Management (ID.AM):** Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy o **ID.AM-08:** Systems, hardware, software, services, and data are managed throughout their life cycles; **Platform Security (PR.PS):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability **o PR.PS-02:** Software is maintained, replaced, and removed commensurate with risk **o PR.PS-03:** Hardware is maintained, replaced, and removed commensurate with risk

Security hardening task	NIST Cybersecurity Framework (CSF 2.0): NIST CSF is risk-based and widely adopted in both public and private sectors.
Multifactor authentication (MFA)	**Identity Management, Authentication, and Access Control (PR.AA):** Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access **PR.AA-03:** Users, services, and hardware are authenticated

Security hardening task	**NIST Cybersecurity Framework (CSF 2.0):** NIST CSF is risk-based and widely adopted in both public and private sectors.
Network access privileges	**Identity Management, Authentication, and Access Control (PR.AA):** Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access **PR.AA-05:** Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties

Security hardening task	NIST Cybersecurity Framework (CSF 2.0): NIST CSF is risk-based and widely adopted in both public and private sectors.
Network log analysis	**Continuous Monitoring (DE.CM):** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events **o DE.CM-01:** Networks and network services are monitored to find potentially adverse events **Platform Security (PR.PS):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability **o PR.PS-04:** Log records are generated and made available for continuous monitoring
Password policies	**Identity Management, Authentication, and Access Control (PR.AA):** Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access **o PR.AA-01:** Identities and credentials for authorized users, services, and hardware are managed by the organization **o PR.AA-03:** Users, services, and hardware are authenticated

Security hardening task	**NIST Cybersecurity Framework (CSF 2.0):** NIST CSF is risk-based and widely adopted in both public and private sectors.
Patch updates	**Platform Security (PR.PS):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability **o PR.PS-02:** Software is maintained, replaced, and removed commensurate with risk
Penetration test (pen test)	**Improvement (ID.IM):** Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions **o ID.IM-02:** Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties **Risk Assessment (ID.RA):** The cybersecurity risk to the organization, assets, and individuals is understood by the organization **o ID.RA-08:** Processes for receiving, analyzing, and responding to vulnerability disclosures are established

Security hardening task	NIST Cybersecurity Framework (CSF 2.0): NIST CSF is risk-based and widely adopted in both public and private sectors.
Port filtering	**Technology Infrastructure Resilience (PR.IR):** Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilienc **o PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage **Platform Security (PR.PS):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability **o PR.PS-01:** Configuration management practices are established and applied
Removing or disabling unused applications and services	**Platform Security (PR.PS):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability **o PR.PS-05:** Installation and execution of unauthorized software are prevented

Security hardening task	**NIST Cybersecurity Framework (CSF 2.0):** NIST CSF is risk-based and widely adopted in both public and private sectors.
Server and data storage backups	Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information **o PR.DS-11**: Backups of data are created, protected, maintained, and tested

Security hardening task	NIST SP 800-53: Used by U.S. government & military, but widely referenced for hardening.	NIST SP 800-53: Related controls	NIST SP 800-53: References
Baseline configurations	**CM-2 Baseline Configuration:** Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change. **CM-6 Configuration Settings:** Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Privacy parameters are parameters impacting the privacy posture of systems, including the parameters required to satisfy other privacy controls. Privacy parameters include settings for access controls, data processing preferences, and processing and retention permissions. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system.	AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18. AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6.	

Security hardening task	**NIST SP 800-53:** Used by U.S. government & military, but widely referenced for hardening.	**NIST SP 800-53: Related controls**	**NIST SP 800-53: References**
Configuration checks	**CM-3 Configuration Change Control:** Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediated vulnerabilities, and unscheduled or unauthorized changes. Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes. For changes that impact privacy risk, the senior agency official for privacy updates privacy impact assessments and system of records notices. For new systems or major upgrades, organizations consider including representatives from the development organizations on the Configuration Control Boards or Change Advisory Boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10. **CM-6 Configuration Settings:** Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Privacy parameters are parameters impacting the privacy posture of systems, including the parameters required to satisfy other privacy controls. Privacy parameters include settings for access controls, data processing preferences, and processing and retention permissions. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system.	CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-6, RA-8, SA-8, SA-10, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11. AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6.	

Security hardening task	**NIST SP 800-53:** Used by U.S. government & military, but widely referenced for hardening.	NIST SP 800-53: Related controls	NIST SP 800-53: References
Disabling unused ports	**CM-7 Least Functionality:** Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk compared to limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and endpoint protection technologies such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA-8, SC-2, and SC-3). **SC-7 Boundary Protection:** Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational systems includes: • Restricting external web traffic to designated web servers within managed interfaces • Prohibiting external traffic that appears to be spoofing internal addresses • Prohibiting internal traffic that appears to be spoofing external addresses SP 800-189 provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third-party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions. Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).	AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC-2, SC-3, SC-7, SC-37, SI-4. 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.	

Security hardening task	**NIST SP 800-53:** Used by U.S. government & military, but widely referenced for hardening.	**NIST SP 800-53: Related controls**	**NIST SP 800-53: References**
Encryption using the latest standards	**SC-12 Cryptographic Key Establishment and Management:** 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 (Cryptographic Module Validation Program) and NIST CAVP (Cryptographic Algorithm Validation Program) provide additional information on validated cryptographic modules and algorithms that can be used in cryptographic key management and establishment. **SC-13 Cryptographic Protection:** 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. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. For example, organizations that need to protect classified information may specify the use of NSA-approved cryptography. Organizations that need to provision and implement digital signatures may specify the use of FIPS-validated cryptography. Cryptography is implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. **SC-28 Protection of Information at Rest:** Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file-share scanning. Integrity protection can be achieved, for example, by implementing write-once-read-many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure offline storage in lieu of online storage.	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 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 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.	NIST CMVP, NIST CAVP

Security hardening task	**NIST SP 800-53:** Used by U.S. government & military, but widely referenced for hardening.	**NIST SP 800-53: Related controls**	**NIST SP 800-53: References**
Firewall maintenance	**SC-7 Boundary Protection:** Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs). Restricting or prohibiting interfaces within organizational systems includes: • Restricting external web traffic to designated web servers within managed interfaces • Prohibiting external traffic that appears to be spoofing internal addresses • Prohibiting internal traffic that appears to be spoofing external addresses SP 800-189 provides additional information on source-address validation techniques to prevent ingress and egress of traffic with spoofed addresses. Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third-party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions. Boundary protection may be implemented as a common control for all or part of an organizational network such that the protected boundary is broader than a single system's authorization boundary. **SC-1(12) Host-based Protection:** Host-based boundary protection mechanisms include host-based firewalls. System components that employ host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.	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.	

Security hardening task	NIST SP 800-53: Used by U.S. government & military, but widely referenced for hardening.	NIST SP 800-53: Related controls	NIST SP 800-53: References
Hardware & software disposal	**MP-6 Media Sanitization:** Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations exercise discretion in employing approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable, or information deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words by obscuring them in a manner equivalent in effectiveness to removing them. NSA standards and policies control the sanitization process for media that contains classified information. NARA policies control the sanitization process for controlled unclassified information. **SA-19 Component Authenticity:** *Withdrawn: Incorporated into SR-12.* **SR-12 Component Disposal:** Data, documentation, tools, or system components can be disposed of at any time during the system development life cycle (not only in the disposal or retirement phase). For example, disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, or partial reuse of components. Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media containing sensitive or proprietary information. Proper disposal of system components also helps prevent such components from entering the gray market. **CM-2(4) Unauthorized Software:** *Withdrawn: Incorporated into CM-7(4).* **CM-7(4) Unauthorized Software — Deny-by-Exception:** Unauthorized software programs can be limited to specific versions or from a specific source. The concept of prohibiting the execution of unauthorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. **CM-7(5) Authorized Software — Allow-by-Exception:** Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized-software process and increase protection against attacks that bypass application-level controls, software programs may be decomposed into and monitored at different levels of detail—applications, application programming interfaces, modules, scripts, system processes, services, kernel functions, registries, drivers, and dynamic-link libraries. Permitting execution of authorized software may also apply to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. Organizations consider verifying the integrity of authorized software using digital signatures, cryptographic checksums, or hash functions. Verification can occur either prior to execution or at system startup. (Identification of authorized URLs for websites is addressed in CA-3(5) and SC-7.)	AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11 MP-6. CM-6, CM-8, CM-10, PL-9, PM-5. CM-2, CM-6, CM-8, CM-10, PL-9, PM-5, SA-10, SC-34, SI-7.	CA-3(5), SC-7.

Security hardening task	**NIST SP 800-53:** Used by U.S. government & military, but widely referenced for hardening.	**NIST SP 800-53: Related controls**	**NIST SP 800-53: References**
Multifactor authentication (MFA)	**IA-2(1) Multi-factor Authentication to Privileged Accounts:** Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: • **Something you know** (e.g., a personal identification number [PIN]) • **Something you have** (e.g., a physical authenticator such as a cryptographic private key) • **Something you are** (e.g., a biometric) Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card / Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (local, network, or remote), privileged accounts are authenticated using multi-factor options appropriate to the level of risk. Organizations can add additional security measures—such as more rigorous authentication mechanisms—for specific types of access. **IA-2(2) Multi-factor Authentication to Non-privileged Accounts:** Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as above. Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card / Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level to provide increased information security. Regardless of the type of access (local, network, or remote), non-privileged accounts are authenticated using multi-factor options appropriate to the level of risk. Organizations can provide additional security measures—such as more rigorous authentication mechanisms—for specific types of access. **IA-2(13) Out-of-band Authentication:** Out-of-band authentication refers to the use of two separate communication paths to identify and authenticate users or devices to an information system. The first path (the in-band path) is used to identify and authenticate users or devices and is generally the path through which information flows. The second path (the out-of-band path) is used to independently verify the authentication and/ or requested action. For example, a user authenticates via a notebook computer to a remote server to which they desire access and requests some action via that path. Subsequently, the server contacts the user via the user's cell phone to verify that the requested action originated from the user. The user may confirm the intended action orally or provide an authentication code via telephone. Out-of-band authentication can be used to mitigate actual or suspected man-in-the-middle attacks. Conditions or criteria for activation include suspicious activities, new threat indicators, elevated threat levels, or the impact or classification level of information in the requested transactions.	AC-5, AC-6. IA-10, IA-11, SC-37.	[FIPS 140-3], [FIPS 201-2], [FIPS 202], [IR 7539], [IR 7676], [IR 7817], [IR 7849], [IR 7870], [IR 7874], [IR 7966], [SP 800-156], [SP 800-166], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [SP 800-79-2]

Security hardening task	**NIST SP 800-53:** Used by U.S. government & military, but widely referenced for hardening.	**NIST SP 800-53: Related controls**	**NIST SP 800-53: References**
Network access privileges	**AC-2 Account Management:** 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 Access Enforcement:** Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family. **AC-6 Least Privilege:** Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.	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. 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. AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38.	

Security hardening task	**NIST SP 800-53:** Used by U.S. government & military, but widely referenced for hardening.	**NIST SP 800-53: Related controls**	**NIST SP 800-53: References**
Network log analysis	**AU-6 Audit Record Review, Analysis, and Reporting:** Audit record review, analysis, and reporting covers information security- and privacy-related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The frequency, scope, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received. **SI-4 System Monitoring:** 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. Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs.	AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7. 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.	
Password policies	**IA-5(1) Password-based Authentication:** 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). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof. **(4) Automated Support for Password Strength Determination:** [Withdrawn: Incorporated into IA-5(1).	IA-6.	

Security hardening task	**NIST SP 800-53:** Used by U.S. government & military, but widely referenced for hardening.	**NIST SP 800-53: Related controls**	**NIST SP 800-53: References**
Patch updates	**SI-2 Flaw Remediation:** The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified. **MA-3(6) Software Updates and Patches:** Maintenance tools using outdated and/or unpatched software can provide a threat vector for adversaries and result in a significant vulnerability for organizations.	CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI-5, SI-7, SI-11. AC-3, AC-6.	[SP 800-88]
Penetration test (pen test)	**CA-8 Penetration Testing:** Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is carried out by teams with demonstrable expertise in network, operating-system, and application-level security. It can validate identified vulnerabilities or determine the degree of resistance of systems under constraints such as time, resources, and skills. By attempting to duplicate adversary actions, penetration testing delivers an in-depth analysis of security- and privacy-related weaknesses or deficiencies and is especially critical when transitioning from older to newer technologies (for example, IPv4 to IPv6). Organizations leverage vulnerability analysis results to plan tests, which may be internal or external and may target hardware, software, or firmware components while exercising both physical and logical controls. A typical process involves a pretest analysis based on full system knowledge, identification of potential vulnerabilities, and targeted testing to gauge exploitability. All parties agree to formal rules of engagement beforehand, correlating them with the tools, techniques, and procedures adversaries might use. Because testing can expose information protected by laws or regulations, contracts or engagement rules stipulate how to safeguard it. Risk assessments determine the necessary independence of testing personnel. **SA-11(5) Penetration Testing:** Under SA-11(5), penetration testing is an assessment methodology in which testers, armed with all available system documentation and operating under defined constraints, attempt to circumvent implemented security and privacy controls. Testers may follow white-box, gray-box, or black-box approaches, using product and system design specifications, source code, and administrator/operator manuals to guide their efforts. The goal is to uncover vulnerabilities arising from implementation errors, misconfigurations, or operational weaknesses. These tests often run alongside automated and manual code reviews to deepen analysis. Any user session data or personally identifiable information captured during testing is handled in accordance with privacy protections.	RA-5, RA-10, SA-11, SR-5, SR-6. CA-8, PM-14, PM-25, PT-2, SA-3, SI-2, SI-6.	

Security hardening task	**NIST SP 800-53:** Used by U.S. government & military, but widely referenced for hardening.	NIST SP 800-53: Related controls	NIST SP 800-53: References
Port filtering	**SC-7(5) Deny by Default — Allow by Exception:** Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to any system connected to an external system. **SC-7(11) Restrict Incoming Communications Traffic:** General source address validation techniques are applied to restrict the use of illegal and unallocated source addresses, as well as source addresses that should only be used within the system. The restriction of incoming communications traffic provides determinations that source and destination address pairs represent authorized or allowed communications. Determinations can be based on the presence of such address pairs in lists of authorized communications, the absence of such address pairs in lists of unauthorized or disallowed pairs, or meeting broader rules for allowed source and destination pairs. Strong authentication of network addresses is not possible without explicit security protocols, and thus addresses can often be spoofed. Additional identity-based incoming traffic restriction methods can be employed, including router access control lists and firewall rules.	AC-3.	
Removing or disabling unused applications and services	**CM-7 Least Functionality:** Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk compared with limiting the services provided by that single component. Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality can also be achieved as part of the fundamental design and development of the system (see SA-8, SC-2, and SC-3). **CM-11 User-installed Software:** If provided the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved app stores. Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization-developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods.	AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC-2, SC-3, SC-7, SC-37, SI-4. AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7.	SA-8, SC-2, SC-3

Security hardening task	NIST SP 800-53: Used by U.S. government & military, but widely referenced for hardening.	NIST SP 800-53: Related controls	NIST SP 800-53: References
Server and data storage backups	**CP-9 System Backup:** System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of system backup information while in transit is addressed by MP-5 and SC-8. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Organizations may be subject to laws, executive orders, directives, regulations, or policies with requirements regarding specific categories of information (e.g., personal health information). Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements. **CP-10 System Recovery and Reconstitution:** Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities; recovery point, recovery time, and reconstitution objectives; and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.	CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.	MP-5, SC-8.