3

المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

Critical Infrastructure Cyber Security Controls

CICSC MAPPING ANNEX

December 2024

CONTENTS

1 INTRODUCTION

Republished courtesy of the National Institute of Standards and Technology (NIST), this document provides additional information relating to the 405 controls included within the Critical Infrastructure Cyber Security Controls (CICSC) that are derived from the following publications:

> Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 800-53 Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5
>
> Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 3. https://doi.org/10.6028/NIST.SP.800-82r3
>
> Joint Task Force (2020) Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B. https://doi.org/10.6028/NIST.SP.800-53B

Where relevant, each control has been mapped to Jordan's National Cybersecurity Framework.

For more information about implementing the controls see the CICSC Guidance. A glossary of key terms is included within CICSC.

2 CONTROL FAMILY: ACCESS CONTROL

Implementation Level | 1

AC-1 Policy and Procedures

Control Context

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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls IA-1, PM-9, PM-24, PS-8, SI-12 .

JNCSF Alignment JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level | 1

AC-2 Account Management

Control Context

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.

Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts. Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.

Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training.

Related Controls 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.

JNCSF Alignment JNCSF-96 Delivery, JNCSF-97 Delivery, JNCSF-139 Operation, JNCSF-140 Operation, JNCSF-141 Operation

Implementation Level 2

AC-2(1) Account Management | Automated System Account Management

Control Context 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.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-2(2) Account Management | Automated Temporary and Emergency Account Management

Control Context

Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

Related Controls

None.

JNCSF Alignment

Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-2(3) Account Management | Disable Accounts

Control Context

Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

Related Controls

None.

JNCSF Alignment

Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-2(4) Account Management | Automated Audit Actions

Control Context

Account management audit records are defined in accordance with AU-2 and reviewed, analyzed, and reported in accordance with AU-6.

Related Controls

AU-2, AU-6.

JNCSF Alignment

Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-2(5) Account Management | Inactivity Logout

Control Context

Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.

Related Controls

AC-11.

JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AC-2(9) Account Management | Restrictions on Use of Shared and Group Accounts

Control Context	Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts.
Related Controls	None.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AC-2(11) Account Management | Usage Conditions

Control Context	Specifying and enforcing usage conditions helps to enforce the principle of least privilege, increase user accountability, and enable effective account monitoring. Account monitoring includes alerts generated if the account is used in violation of organizational parameters. Organizations can describe specific conditions or circumstances under which system accounts can be used, such as by restricting usage to certain days of the week, time of day, or specific durations of time.
Related Controls	None.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AC-2(12) Account Management | Account Monitoring for Atypical Usage

Control Context	Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress. Account monitoring may inadvertently create privacy risks since data collected to identify atypical usage may reveal previously unknown information about the behavior of individuals. Organizations assess and document privacy risks from monitoring accounts for atypical usage in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.
Related Controls	AU-6, AU-7, CA-7, IR-8, SI-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-2(13) Account Management | Disable Accounts for High-risk Individuals

Control Context 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.

Related Controls AU-6, SI-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

AC-3 Access Enforcement

Control Context 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.

Related Controls 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,

JNCSF Alignment JNCSF-440 Foundational

Implementation Level 3

AC-3(11) Access Enforcement | Restrict Access to Specific Information Types

Control Context Restricting access to specific information is intended to provide flexibility regarding access control of specific information types within a system. For example, role-based access could be employed to allow access to only a specific type of personally identifiable information within a database rather than allowing access to the database in its entirety. Other examples include restricting access to cryptographic keys, authentication information, and selected system information.

Related Controls	CM-8, CM-12, CM-13, PM-5.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-4 Information Flow Enforcement

Control Context

Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between connected systems. Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e. allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e. hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 32 primarily address cross-domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf products. Information flow enforcement also applies to control plane traffic (e.g. routing and DNS).

Related Controls	AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AC-4(4) Information Flow Enforcement | Flow Control of Encrypted Information

Control Context Flow control mechanisms include content checking, security policy filters, and data type identifiers. The term encryption is extended to cover encoded data not recognized by filtering mechanisms.

Related Controls SI-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-5 Separation of Duties

Control Context Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. Separation of duties is enforced through the account management activities in AC-2, access control mechanisms in AC-3, and identity management activities in IA-2, IA-4, and IA-12.

Related Controls 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.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-6 Least Privilege

Control Context 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.

Related Controls AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38.

JNCSF Alignment JNCSF-102 - Delivery

Implementation Level 2

AC-6(1) Least Privilege | Authorize Access to Security Functions

Control Context Security functions include establishing system accounts, configuring access authorizations (i.e. permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.

Related Controls AC-17, AC-18, AC-19, AU-9, PE-2.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-6(2) Least Privilege | Non-privileged Access for Nonsecurity Functions

Control Context Requiring the use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies, such as role-based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

Related Controls AC-17, AC-18, AC-19, PL-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AC-6(3) Least Privilege | Network Access to Privileged Commands

Control Context Network access is any access across a network connection in lieu of local access (i.e. user being physically present at the device).

Related Controls	AC-17, AC-18, AC-19.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-6(5) Least Privilege | Privileged Accounts

Control Context

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.

Related Controls	IA-2, MA-3, MA-4.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-6(7) Least Privilege | Review of User Privileges

Control Context

The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

Related Controls	CA-7.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-6(9) Least Privilege | Log Use of Privileged Functions

Control Context

The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and, in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

Related Controls AU-2, AU-3, AU-12.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-6(10) Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions

Control Context Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. Preventing non-privileged users from executing privileged functions is enforced by AC-3.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

AC-7 Unsuccessful Logon Attempts

Control Context The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined, organization-defined time period. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels. Organization-defined actions that may be taken when the number of allowed consecutive invalid logon attempts is exceeded include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address. If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, organizations consider a combination of other actions to help prevent brute force attacks. In addition to the above, organizations can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or need.

Related Controls AC-2, AC-9, AU-2, AU-6, IA-5.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

AC-8 System Use Notification

Control Context System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon interfaces with human users. Notifications are not required when human interfaces do not exist. Based on an assessment of risk, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network logon. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users. Organizations consult with the privacy office for input regarding privacy messaging and the Office of the General Counsel or organizational equivalent for legal review and approval of warning banner content.

Related Controls AC-14, PL-4, SI-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AC-10 Concurrent Session Control

Control Context Organizations may define the maximum number of concurrent sessions for system accounts globally, by account type, by account, or any combination thereof. For example, organizations may limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications. Concurrent session control addresses concurrent sessions for system accounts. It does not, however, address concurrent sessions by single users via multiple system accounts.

Related Controls SC-23.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

AC-11 Device Lock

Control Context Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g. via a Bluetooth-enabled device or dongle). User-initiated device locking is behavior or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.

Related Controls AC-2, AC-7, IA-11, PL-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-11(1) Device Lock | Pattern-hiding Displays

Control Context The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-12 Session Termination

Control Context Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions (i.e. network disconnect)). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user’s logical session except for those processes that are specifically created by the user (i.e. session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

Related Controls MA-4, SC-10, SC-23.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

AC-14 Permitted Actions Without Identification or Authentication

Control Context Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication are not required for the specified user actions. Organizations may allow a limited number of user actions without identification or authentication, including when individuals access public websites or other publicly accessible Government systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations identify actions that normally require identification or authentication but may, under certain circumstances, allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. Permitting actions without identification or authentication does not apply to situations where identification and authentication have already occurred and are not repeated but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication, and therefore, the value for the assignment operation can be none.

Related Controls AC-8, IA-2, PL-2.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AC-16 Security and Privacy Attributes

Control Context Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures, such as records, buffers, tables, files, inter-process pipes, and communications ports. Security attributes, a form of metadata, are abstractions that represent the basic properties or characteristics of active and passive entities with respect to safeguarding information. Privacy attributes, which may be used independently or in conjunction with security attributes, represent the basic properties or characteristics of active or passive entities with respect to the management of personally identifiable information. Attributes can be either explicitly or implicitly associated with the information contained in organizational systems or system components.

Attributes may be associated with active entities (i.e. subjects) that have the potential to send or receive information, cause information to flow among objects, or change the system state. These attributes may also be associated with passive entities (i.e. objects) that contain or receive information. The association of attributes to subjects and objects by a system is referred to as binding and is inclusive of setting the attribute value and the attribute type. Attributes, when bound to data or information, permit the enforcement of security and privacy policies for access control and information flow control, including data retention limits, permitted uses of personally identifiable information, and identification of personal information within data objects. Such enforcement occurs through organizational processes or system functions or mechanisms. The binding techniques implemented by systems affect the strength of attribute binding to information. Binding strength and the assurance associated with binding techniques play important parts in the trust that organizations have in the information flow enforcement process. The binding techniques affect the number and degree of additional reviews required by organizations. The content or assigned values of attributes can directly affect the ability of individuals to access organizational information.

Organizations can define the types of attributes needed for systems to support missions or business functions. There are many values that can be assigned to a security attribute. By specifying the permitted attribute ranges and values, organizations ensure that attribute values are meaningful and relevant. Labelling refers to the association of attributes with the subjects and objects represented by the internal data structures within systems. This facilitates system-based enforcement of information security and privacy policies. Labels include classification of information in accordance with legal and compliance requirements (e.g. top secret, secret, confidential, controlled unclassified), information impact level; high value asset information, access authorizations, nationality; data life cycle protection (i.e. encryption and data expiration), personally identifiable information processing permissions, including individual consent to personally identifiable information processing, and contractor affiliation. A related term to labelling is marking. Marking refers to the association of attributes with objects in a human-readable form and displayed on system media. Marking enables manual, procedural, or process-based enforcement of information security and privacy policies. Security and privacy labels may have the same value as media markings (e.g. top secret, secret, confidential). See MP-3 (Media Marking)

Related Controls AC-3, AC-4, AC-6, AC-21, AC-25, AU-2, AU-10, MP-3, PE-22, PT-2, PT-3, PT-4, SC-11, SC-16, SI-12, SI-18.

JNCSF Alignment JNCSF-148 – Operation, JNCSF-150 - Operation

Implementation Level I

AC-17 Remote Access

Control Context Remote access is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the ability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. Authorization of each remote access type addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use information exchange and system connection security agreements to manage remote access connections to other systems, such agreements are addressed as part of CA-3. Enforcing access restrictions for remote access is addressed via AC-3.

Related Controls 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.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-17(1) Remote Access | Monitoring and Control

Control Context Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.

Related Controls AU-2, AU-6, AU-12, AU-14.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-17(2) Remote Access | Protection of Confidentiality and Integrity Using Encryption

Control Context Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

Related Controls SC-8, SC-12, SC-13.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-17(3) Remote Access | Managed Access Control Points

Control Context Organizations consider the NCSC-JO requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.

Related Controls SC-7.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-17(4) Remote Access | Privileged Commands and Access

Control Context Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.

Related Controls AC-6, SC-12, SC-13.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AC-17(9) Remote Access | Disconnect or Disable Access

Control Context The speed of system disconnect or disablement varies based on the criticality of missions or business functions and the need to eliminate immediate or future remote access to systems.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AC-17(10) Remote Access | Authenticate Remote Commands

Control Context Authenticating remote commands protects against unauthorized commands and the replay of authorized commands. The ability to authenticate remote commands is important for remote systems for which loss, malfunction, misdirection, or exploitation would have immediate or serious consequences, such as injury, death, property damage, loss of high value assets, failure of mission or business functions, or compromise of classified or controlled unclassified information. Authentication mechanisms for remote commands ensure that systems accept and execute commands in the order intended, execute only authorized commands, and reject unauthorized commands. Cryptographic mechanisms can be used, for example, to authenticate remote commands.

Related Controls SC-12, SC-13, SC-23.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | 1 |

AC-18 Wireless Access

Control Context: Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols that provide authenticator protection and mutual authentication.

Related Controls: AC-2, AC-3, AC-17, AC-19, CA-9, CM-7, IA-2, IA-3, IA-8, PL-4, SC-40, SC-43, SI-4.

JNCSF Alignment: JNCSF-159 Operation, JNCSF-160 Operation

Implementation Level | 2 |

AC-18(1) Wireless Access | Authentication and Encryption

Control Context: Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls: SC-8, SC-12, SC-13.

JNCSF Alignment: Additional to Jordan's National Cybersecurity Framework

Implementation Level | 2 |

AC-18(3) Wireless Access | Disable Wireless Networking

Control Context: Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls: None.

JNCSF Alignment: Additional to Jordan's National Cybersecurity Framework

Implementation Level | 3 |

AC-18(4) Wireless Access | Restrict Configurations by Users

Control Context: Organizational authorizations to allow selected users to configure wireless networking capabilities are enforced, in part, by the access enforcement mechanisms employed within organizational systems.

Related Controls SC-7, SC-15.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AC-18(5) Wireless Access | Antennas and Transmission Power Levels

Control Context Actions that may be taken to limit unauthorized use of wireless communications outside of organization-controlled boundaries include reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be captured outside of the physical perimeters of the organization, employing measures such as emissions security to control wireless emanations, and using directional or beamforming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such mitigating actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational systems as well as other systems that may be operating in the area.

Related Controls PE-19.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

AC-19 Access Control for Mobile Devices

Control Context A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending on the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting information and systems.

Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware.

Usage restrictions and authorization to connect may vary among organizational systems. For example, the organization may authorize the connection of mobile devices to its network and impose a set of usage restrictions, while a system owner may withhold authorization for mobile device connection to specific applications or impose additional usage restrictions before allowing mobile device connections to a system. Adequate security for mobile devices goes beyond the requirements specified in AC-19. Many safeguards for mobile devices are reflected in other controls. AC-20 addresses mobile devices that are not organization-controlled.

Related Controls 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.

JNCSF Alignment JNCSF-105 Delivery, JNCSF-162 Operation, JNCSF-163 Operation, JNCSF-451 Foundational

Implementation Level 2

AC-19(5) Access Control for Mobile Devices | Full Device or Container-based Encryption

Control Context Container-based encryption provides a more fine-grained approach to data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields.

Related Controls SC-12, SC-13, SC-28.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

AC-20 Use of External Systems

Control Context External systems are systems that are used by but not part of organizational systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. External systems include personally owned systems, components, or devices; privately owned computing and communications devices in commercial or public facilities; systems owned or controlled by non-government organizations; systems managed by contractors; and government information systems that are not owned by, operated by, or under the direct supervision or authority of the organization. External systems also include systems owned or operated by other components within the same organization and systems within the organization with different authorization boundaries. Organizations have the option to prohibit the use of any type of external system or prohibit the use of specified types of external systems, (e.g. prohibit the use of any external system that is not organizationally owned or prohibit the use of personally-owned systems).

For some external systems (i.e. systems operated by other organizations), the trust relationships that have been established between those organizations and the originating organization may be such that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing information exchange agreements (either implicit or explicit) established between organizations or components or when such agreements are specified by applicable laws, executive orders, directives, regulations, policies, or standards. Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to organizational systems and over which organizations have the authority to impose specific rules of behavior regarding system access. Restrictions that organizations impose on authorized individuals need not be uniform, as the restrictions may vary depending on trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

External systems used to access public interfaces to organizational systems are outside the scope of AC-20. Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems. If the terms and conditions with the owners of the external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

Related Controls AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7.

JNCSF Alignment JNCSF-452 Foundational, JNCSF-453 Foundational

Implementation Level 2

AC-20(1) Use of External Systems | Limits on Authorized Use

Control Context Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

Related Controls CA-2.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-20(2) Use of External Systems | Portable Storage Devices — Restricted Use

Control Context Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.

Related Controls	MP-7, SC-41.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AC-21 Information Sharing

Control Context

Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

Related Controls	AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15.
JNCSF Alignment	JNCSF-454 Foundational

Implementation Level 1

AC-22 Publicly Accessible Content

Control Context

In accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including information protected under the PRIVACT and proprietary information. Publicly accessible content addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Posting information on non-organizational systems (e.g. non-organizational public websites, forums, and social media) is covered by organizational policy. While organizations may have individuals who are responsible for developing and implementing policies about the information that can be made publicly accessible, publicly accessible content addresses the management of the individuals who make such information publicly accessible.

Related Controls	AC-3, AT-2, AT-3, AU-13.
JNCSF Alignment	JNCSF-29 Development, JNCSF-455 Foundational, JNCSF-458 Foundational

Implementation Level 2

AC-23 Data Mining Protection

Control Context

Data mining is an analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery. Data storage objects include database records and database fields. Sensitive information can be extracted from data mining operations. When information is personally identifiable information, it may lead to unanticipated revelations about individuals and give rise to privacy risks. Prior to performing data mining activities, organizations determine whether such activities are authorized. Organizations may be subject to applicable laws, executive orders, directives, regulations, or policies that address data mining requirements. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Data mining prevention and detection techniques include limiting the number and frequency of database queries to increase the work factor needed to determine the contents of databases, limiting types of responses provided to database queries, applying differential privacy techniques or homomorphic encryption, and notifying personnel when atypical database queries or accesses occur. Data mining protection focuses on protecting information from data mining while such information resides in organizational data stores. In contrast, AU-13 focuses on monitoring for organizational information that may have been mined or otherwise obtained from data stores and is available as open-source information residing on external sites, such as social networking or social media websites.

Data mining protection requires organizations to identify appropriate techniques to prevent and detect unnecessary or unauthorized data mining. Data mining can be used by an insider to collect organizational information for the purpose of exfiltration

Related Controls PM-12, PT-2.

JNCSF Alignment JNCSF-165 - Operation

3 CONTROL FAMILY: AWARENESS AND TRAINING

Implementation Level	1

AT-1 Policy and Procedures

Control Context

Awareness and training policy and procedures address the controls in the AT 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 awareness and training 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 that reflect 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to awareness and training policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls PM-9, PS-8, SI-12.

JNCSF Alignment JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level	1

AT-2 Literacy Training and Awareness

Control Context

Organizations provide basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users. Organizations determine the content of literacy training and awareness based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g. telework). The content includes an understanding of the need for security and privacy as well as actions by users to maintain security and personal privacy and to respond to suspected incidents. The content addresses the need for operations security and the handling of personally identifiable information.

Awareness techniques include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices from organizational officials, and conducting awareness events. Literacy training after the initial training described in AT-2a.1 is conducted at a minimum frequency consistent with applicable laws, directives, regulations, and policies. Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training. Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16.

JNCSF Alignment JNCSF-459 Foundational, JNCSF-460 Foundational

Implementation Level 1

AT-2(2) Literacy Training and Awareness | Insider Threat

Control Context Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices. Literacy training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role. For example, training for managers may be focused on changes in the behavior of team members, while training for employees may be focused on more general observations.

Related Controls PM-12.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AT-2(3) Literacy Training and Awareness | Social Engineering and Mining

Control Context Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Literacy training includes information on how to communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AT-2(4) Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior

Control Context

A well-trained workforce provides another organizational control that can be employed as part of a defense-in-depth strategy to protect against malicious code coming into organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email (e.g. receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender that appears to be from a known sponsor or contractor). Personnel are also trained on how to respond to suspicious email or web communications. For this process to work effectively, personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in systems can provide organizations with early warning for the presence of malicious code. Recognition of anomalous behavior by organizational personnel can supplement malicious code detection and protection tools and systems employed by organizations.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

AT-3 Role-based Training

Control Context

Organizations determine the content of training based on the assigned roles and responsibilities of individuals as well as the security and privacy requirements of organizations and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties. Roles that may require role-based training include senior leaders or management officials (e.g. head of agency/chief executive officer, chief information officer, senior accountable official for risk management, senior agency information security officer, senior agency official for privacy), system owners; authorizing officials; system security officers; privacy officers; acquisition and procurement officials; enterprise architects; systems engineers; software developers; systems security engineers; privacy engineers; system, network, and database administrators; auditors; personnel conducting configuration management activities; personnel performing verification and validation activities; personnel with access to system-level software; control assessors; personnel with contingency planning and incident response duties; personnel with privacy management responsibilities; and personnel with access to personally identifiable information.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of organizational security and privacy programs. Role-based training also applies to contractors who provide services to government agencies. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Updating role-based training on a regular basis helps to ensure that the content remains relevant and effective. Events that may precipitate an update to role-based training content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, IR-9, PL-4, PM-13, PM-23, PS-7, PS-9, SA-3, SA-8, SA-11, SA-16, SR-5, SR-6, SR-11.

JNCSF Alignment JNCSF-461 Foundational, JNCSF-462 Foundational

Implementation Level I

AT-4 Training Records

Control Context Documentation for specialized training may be maintained by individual supervisors at the discretion of the organization. Local laws or regulators should provides guidance on records retention for CNI entitites.

Related Controls AT-2, AT-3, CP-3, IR-2, PM-14, SI-12.

JNCSF Alignment JNCSF-465 Foundational

4 CONTROL FAMILY: AUDIT AND ACCOUNTABILITY

Implementation Level I

AU-1 Policy and Procedures

Control Context

Audit and accountability policy and procedures address the controls in the AU 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 audit and accountability 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 that reflect 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to audit and accountability policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls PM-9, PS-8, SI-12.

JNCSF Alignment JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level I

AU-2 Event Logging

Control Context

An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, organizations consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.

To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. The types of events that organizations desire to be logged may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization. Organizations consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the logging event is based on patterns or time of usage.

Event logging requirements, including the need to log specific event types, may be referenced in other controls and control enhancements. Organizations include event types that are required by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of event logging is an important part of a monitoring and auditing capability and can identify the root causes of problems. When defining event types, organizations consider the logging necessary to cover related event types, such as the steps in distributed, transaction-based processes and the actions that occur in service-oriented architectures.

Related Controls AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.

JNCSF Alignment JNCSF-167 Operation, JNCSF-168 Operation

Implementation Level 1

AU-3 Content of Audit Records

Control Context Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f) . Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

Related Controls AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7, SI-11.

JNCSF Alignment JNCSF-30 Development

Implementation Level 2

AU-3(1) Content of Audit Records | Additional Audit Information

Control Context The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records including, but not limited to, access control or flow control rules invoked and individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. This facilitates the use of audit trails and audit logs by not including information in audit records that could potentially be misleading, make it more difficult to locate information of interest, or increase the risk to individuals' privacy.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AU-3(3) Content of Audit Records | Limit Personally Identifiable Information Elements

Control Context Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related Controls RA-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

AU-4 Audit Log Storage Capacity

Control Context Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.

Related Controls AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.

JNCSF Alignment JNCSF-170 Operation

Implementation Level 2

AU-4(1) Audit Log Storage Capacity | Transfer to Alternate Storage

Control Context Audit log transfer, also known as off-loading, is a common process in systems with limited audit log storage capacity and thus supports availability of the audit logs. The initial audit log storage is only used in a transitory fashion until the system can communicate with the secondary or alternate system allocated to audit log storage, at which point the audit logs are transferred. Transferring audit logs to alternate storage is similar to AU-9(2) in that audit logs are transferred to a different entity. However, the purpose of selecting AU-9(2) is to protect the confidentiality and integrity of audit records. Organizations can select either control enhancement to obtain the benefit of increased audit log storage capacity and preserving the confidentiality, integrity, and availability of audit records and logs.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

AU-5 Response to Audit Logging Process Failures

Control Context Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization-defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e. the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e. all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

Related Controls AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.

JNCSF Alignment JNCSF-171 Operation, JNCSF-172 Operation

Implementation Level 3

AU-5(1) Response to Audit Logging Process Failures | Storage Capacity Warning

Control Context Organizations may have multiple audit log storage repositories distributed across multiple system components with each repository having different storage volume capacities.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AU-5(2) Response to Audit Logging Process Failures | Real-time Alerts

Control Context Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e. the time from event detection to alert occurs in seconds or less).

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AU-5(3) Response to Audit Logging Process Failures | Configurable Traffic Volume Thresholds

Control Context Organizations have the capability to reject or delay the processing of network communications traffic if audit logging information about such traffic is determined to exceed the storage capacity of the system audit logging function. The rejection or delay response is triggered by the established organizational traffic volume thresholds that can be adjusted based on changes to audit log storage capacity.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AU-5(4) Response to Audit Logging Process Failures | Shutdown on Failure

Control Context Organizations determine the types of audit logging failures that can trigger automatic system shutdowns or degraded operations. Because of the importance of ensuring mission and business continuity, organizations may determine that the nature of the audit logging failure is not so severe that it warrants a complete shutdown of the system supporting the core organizational mission and business functions. In those instances, partial system shutdowns or operating in a degraded mode with reduced capability may be viable alternatives.

Related Controls AU-15.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AU-5(5) Response to Audit Logging Process Failures | Alternate Audit Logging Capability

Control Context Since an alternate audit logging capability may be a short-term protection solution employed until the failure in the primary audit logging capability is corrected, organizations may determine that the alternate audit logging capability need only provide a subset of the primary audit logging functionality that is impacted by the failure.

Related Controls AU-9.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

AU-6 Audit Record Review, Analysis, and Reporting

Control Context 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.

Related Controls 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.

JNCSF Alignment JNCSF-173 Operation

Implementation Level 2

AU-6(1) Audit Record Review, Analysis, and Reporting | Automated Process Integration

Control Context Organizational processes that benefit from integrated audit record review, analysis, and reporting include incident response, continuous monitoring, contingency planning, investigation and response to suspicious activities, and Inspector General audits.

Related Controls PM-7.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | 3

AU-6(3) Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories

Control Context Organization-wide situational awareness includes awareness across all three levels of risk management (i.e. organizational level, mission/business process level, and information system level) and supports cross-organization awareness.

Related Controls AU-12, IR-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | 2

AU-6(4) Audit Record Review, Analysis, and Reporting | Central Review and Analysis

Control Context Automated mechanisms for centralized reviews and analyses include Security Information and Event Management products.

Related Controls AU-2, AU-12.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | 3

AU-6(5) Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records

Control Context Integrated analysis of audit records does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, integrated analysis requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. Security Information and Event Management tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans of the system and in correlating attack detection events with scanning results. Correlation with performance data can uncover denial-of-service attacks or other types of attacks that result in the unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.

Related Controls AU-12, IR-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AU-6(6) Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring

Control Context The correlation of physical audit record information and the audit records from systems may assist organizations in identifying suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identity for logical access to certain systems with the additional physical security information that the individual was present at the facility when the logical access occurred may be useful in investigations.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AU-6(7) Audit Record Review, Analysis, and Reporting | Permitted Actions

Control Context Organizations specify permitted actions for system processes, roles, and users associated with the review, analysis, and reporting of audit records through system account management activities. Specifying permitted actions on audit record information is a way to enforce the principle of least privilege. Permitted actions are enforced by the system and include read, write, execute, append, and delete.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AU-6(8) Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands

Control Context Full text analysis of privileged commands requires a distinct environment for the analysis of audit record information related to privileged users without compromising such information on the system where the users have elevated privileges, including the capability to execute privileged commands. Full text analysis refers to analysis that considers the full text of privileged commands (i.e. commands and parameters) as opposed to analysis that considers only the name of the command. Full text analysis includes the use of pattern matching and heuristics.

Related Controls AU-3, AU-9, AU-11, AU-12.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AU-6(9) Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources

Control Context Nontechnical sources include records that document organizational policy violations related to harassment incidents and the improper use of information assets. Such information can lead to a directed analytical effort to detect potential malicious insider activity. Organizations limit access to information that is available from nontechnical sources due to its sensitive nature. Limited access minimizes the potential for inadvertent release of privacy-related information to individuals who do not have a need to know. The correlation of information from nontechnical sources with audit record information generally occurs only when individuals are suspected of being involved in an incident. Organizations obtain legal advice prior to initiating such actions.

Related Controls PM-12.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AU-7 Audit Record Reduction and Report Generation

Control Context Audit record reduction is a process that manipulates collected audit log information and organizes it into a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities that conduct audit logging activities. The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be an issue if the granularity of the timestamp in the record is insufficient.

Related Controls AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, AU-16, CM-5, IA-5, IR-4, PM-12, SI-4.

JNCSF Alignment JNCSF-175 Operation, JNCSF-176 Operation

Implementation Level 2

AU-7(1) Audit Record Reduction and Report Generation | Automatic Processing

Control Context

Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure. Organizations may define event criteria to any degree of granularity required, such as locations selectable by a general networking location or by specific system component.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

AU-8 Time Stamps

Control Context

Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g. clocks synchronizing within hundreds of milliseconds or tens of milliseconds). Organizations may define different time granularities for different system components. Time service can be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

Related Controls AU-3, AU-12, AU-14, SC-45.

JNCSF Alignment JNCSF-177 Operation, JNCSF-183 Operation

Implementation Level 1

AU-9 Protection of Audit Information

Control Context

Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.

Related Controls AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4.

JNCSF Alignment JNCSF-423 Operation

Implementation Level 3

AU-9(2) Protection of Audit Information | Store on Separate Physical Systems or Components

Control Context Storing audit records in a repository separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organization-wide activity. Storing audit records on separate systems or components applies to initial generation as well as backup or long-term storage of audit records.

Related Controls AU-4, AU-5.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AU-9(3) Protection of Audit Information | Cryptographic Protection

Control Context Cryptographic mechanisms used for protecting the integrity of audit information include signed hash functions using asymmetric cryptography. This enables the distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Related Controls AU-10, SC-12, SC-13.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

AU-9(4) Protection of Audit Information | Access by Subset of Privileged Users

Control Context Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

Related Controls AC-5.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AU-10 Non-repudiation

Control Context Types of individual actions covered by non-repudiation include creating information, sending and receiving messages, and approving information. Non-repudiation protects against claims by authors of not having authored certain documents, senders of not having transmitted messages, receivers of not having received messages, and signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from an individual or if an individual took specific actions (e.g. sending an email, signing a contract, approving a procurement request, or receiving specific information). Organizations obtain non-repudiation services by employing various techniques or mechanisms, including digital signatures and digital message receipts.

Related Controls AU-9, PM-12, SA-8, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23.

JNCSF Alignment JNCSF-178 Operation

Implementation Level 1

AU-11 Audit Record Retention

Control Context Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes the retention and availability of audit records relative to National Cyber Security Law. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. Local laws and regulators should provide guidance on records retention.

Related Controls AU-2, AU-4, AU-5, AU-6, AU-9, AU-14, MP-6, RA-5, SI-12.

JNCSF Alignment JNCSF-179 Operation

Implementation Level 1

AU-12 Audit Record Generation

Control Context Audit records can be generated from many different system components. The event types specified in AU-2d are the event types for which audit logs are to be generated and are a subset of all event types for which the system can generate audit records.

Related Controls AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-14, CM-5, MA-4, MP-4, PM-12, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10.

JNCSF Alignment	JNCSF-30 Development, JNCSF-108 Delivery, JNCSF-466 Foundational

Implementation Level 3

AU-12(1) Audit Record Generation | System-wide and Time-correlated Audit Trail

Control Context	Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.
Related Controls	AU-8, SC-45.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

AU-12(3) Audit Record Generation | Changes by Authorized Individuals

Control Context	Permitting authorized individuals to make changes to system logging enables organizations to extend or limit logging as necessary to meet organizational requirements. Logging that is limited to conserve system resources may be extended (either temporarily or permanently) to address certain threat situations. In addition, logging may be limited to a specific set of event types to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which logging actions are changed (e.g. near real-time, within minutes, or within hours).
Related Controls	AC-3.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

5 CONTROL FAMILY: SECURITY ASSESSMENT AND AUTHORISATION

Implementation Level | I

CA-1 Policy and Procedures

Control Context

Assessment, authorization, and monitoring policy and procedures address the controls in the CA 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 assessment, authorization, and monitoring 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 that reflect 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to assessment, authorization, and monitoring policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls

PM-9, PS-8, SI-12.

JNCSF Alignment

JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level | I

CA-2 Control Assessments

Control Context

Organizations ensure that control assessors possess the required skills and technical expertise to develop effective assessment plans and to conduct assessments of system-specific, hybrid, common, and program management controls, as appropriate. The required skills include general knowledge of risk management concepts and approaches as well as comprehensive knowledge of and experience with the hardware, software, and firmware system components implemented.

Organizations assess controls in systems and the environments in which those systems operate as part of initial and ongoing authorizations, continuous monitoring, annual assessments, system design and development, systems security engineering, privacy engineering, and the system development life cycle. Assessments help to ensure that organizations meet information security and privacy requirements, identify weaknesses and deficiencies in the system design and development process, provide essential information needed to make risk-based decisions as part of authorization processes, and comply with vulnerability mitigation procedures. Organizations conduct assessments on the implemented controls as documented in security and privacy plans. Assessments can also be conducted throughout the system development life cycle as part of systems engineering and systems security engineering processes. The design for controls can be assessed as RFPs are developed, responses assessed, and design reviews conducted. If a design to implement controls and subsequent implementation in accordance with the design are assessed during development, the final control testing can be a simple confirmation utilizing previously completed control assessment and aggregating the outcomes.

Organizations may develop a single, consolidated security and privacy assessment plan for the system or maintain separate plans. A consolidated assessment plan clearly delineates the roles and responsibilities for control assessment. If multiple organizations participate in assessing a system, a coordinated approach can reduce redundancies and associated costs.

Organizations can use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security and privacy posture of systems during the system life cycle. Assessment reports document assessment results in sufficient detail, as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements. Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, senior agency officials for privacy, senior agency information security officers, and authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations, continuous monitoring, systems engineering processes, or system development life cycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits, including audits by external entities such as regulatory agencies, are outside of the scope of CA-2.

Related Controls AC-20, CA-5, CA-6, CA-7, PM-9, RA-5, RA-10, SA-11, SC-38, SI-3, SI-12, SR-2, SR-3.

JNCSF Alignment JNCSF-468 Foundational, JNCSF-469 Foundational, JNCSF-470 Foundational

Implementation Level 2

CA-2(1) Control Assessments | Independent Assessors

Control Context Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments can be obtained from elements within organizations or be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. Assessor independence determination includes whether contracted assessment services have sufficient independence, such as when system owners are not directly involved in contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, having independent assessors is analogous to having independent SMEs involved in design reviews.

When organizations that own the systems are small or the structures of the organizations require that assessments be conducted by individuals that are in the developmental, operational, or management chain of the system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Assessments performed for purposes other than to support authorization decisions are more likely to be useable for such decisions when performed by assessors with sufficient independence, thereby reducing the need to repeat assessments.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CA-2(2) Control Assessments | Specialized Assessments

Control Context Organizations can conduct specialized assessments, including verification and validation, system monitoring, insider threat assessments, malicious user testing, and other forms of testing. These assessments can improve readiness by exercising organizational capabilities and indicating current levels of performance as a means of focusing actions to improve security and privacy. Organizations conduct specialized assessments in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can include vulnerabilities uncovered during assessments into vulnerability remediation processes. Specialized assessments can also be conducted early in the system development life cycle (e.g. during initial design, development, and unit testing).

Related Controls PE-3, SI-2.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | 1 |

CA-3 Information Exchange

Control Context

System information exchange requirements apply to information exchanges between two or more systems. System information exchanges include connections via leased lines or virtual private networks, connections to internet service providers, database sharing or exchanges of database transaction information, connections and exchanges with cloud services, exchanges via web-based services, or exchanges of files via file transfer protocols, network protocols (e.g. IPv4, IPv6), email, or other organization-to-organization communications. Organizations consider the risk related to new or increased threats that may be introduced when systems exchange information with other systems that may have different security and privacy requirements and controls. This includes systems within the same organization and systems that are external to the organization. A joint authorization of the systems exchanging information, as described in CA-6(1) or CA-6(2), may help to communicate and reduce risk.

Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g. government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system. If systems that exchange information have the same authorizing official, organizations need not develop agreements. Instead, the interface characteristics between the systems (e.g. how the information is being exchanged. how the information is protected) are described in the respective security and privacy plans. If the systems that exchange information have different authorizing officials within the same organization, the organizations can develop agreements or provide the same information that would be provided in the appropriate agreement type from CA-3a in the respective security and privacy plans for the systems. Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between government agencies and non-government organizations (including service providers, contractors, system developers, and system integrators). Risk considerations include systems that share the same networks.

Related Controls AC-4, AC-20, AU-16, CA-6, IA-3, IR-4, PL-2, PT-7, RA-3, SA-9, SC-7, SI-12.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | 3 |

CA-3(6) Information Exchange | Transfer Authorizations

Control Context

To prevent unauthorized individuals and systems from making information transfers to protected systems, the protected system verifies—via independent means— whether the individual or system attempting to transfer information is authorized to do so. Verification of the authorization to transfer information also applies to control plane traffic (e.g. routing and DNS) and services (e.g. authenticated SMTP relays).

Related Controls AC-2, AC-3, AC-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | I

CA-5 Plan of Action and Milestones

Control Context Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are required in authorization packages and subject to government reporting requirements established by regulator

Related Controls CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12.

JNCSF Alignment JNCSF-471 Foundational

Implementation Level | I

CA-6 Authorization

Control Context Authorizations are official management decisions by senior officials to authorize operation of systems, authorize the use of common controls for inheritance by organizational systems, and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon controls. Authorizing officials provide budgetary oversight for organizational systems and common controls or assume responsibility for the mission and business functions supported by those systems or common controls. The authorization process is a government responsibility, and therefore, authorizing officials must be government employees. Authorizing officials are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems. Non-government organizations may have similar processes to authorize systems and senior officials that assume the authorization role and associated responsibilities.

Authorizing officials issue ongoing authorizations of systems based on evidence produced from implemented continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes. Through the employment of comprehensive continuous monitoring processes, the information contained in authorization packages (i.e. security and privacy plans, assessment reports, and plans of action and milestones) is updated on an ongoing basis. This provides authorizing officials, common control providers, and system owners with an up-to-date status of the security and privacy posture of their systems, controls, and operating environments. To reduce the cost of reauthorization, authorizing officials can leverage the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

Related Controls CA-2, CA-3, CA-7, PM-9, PM-10, RA-3, SA-10, SI-12.

JNCSF Alignment JNCSF-6 Security in Architecture and Portfolio, JNCSF-109 Delivery, JNCSF-189 Operation

Implementation Level 1

CA-7 Continuous Monitoring

Control Context

Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives organizational officials the ability to make effective and timely risk management decisions, including ongoing authorization decisions.

Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems. Monitoring requirements, including the need for specific monitoring, may be referenced in other controls and control enhancements, such as AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PM-31, PS-7e, SA-9c, SR-4, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b, and SI-4.

Related Controls

AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-7, PT-7, RA-3, RA-5, RA-7, RA-10, SA-8, SA

JNCSF Alignment

JNCSF-190 Operation

Implementation Level 2

CA-7(1) Continuous Monitoring | Independent Assessment

Control Context

Organizations maximize the value of control assessments by requiring that assessments be conducted by assessors with appropriate levels of independence. The level of required independence is based on organizational continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in advocacy positions for the organizations acquiring their services.

Related Controls

None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CA-7(4) Continuous Monitoring | Risk Monitoring

Control Context Risk monitoring is informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CA-8 Penetration Testing

Control Context 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 conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies. Penetration testing is especially important when organizations are transitioning from older technologies to newer technologies (e.g. transitioning from IPv4 to IPv6 network protocols).

Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes a pretest analysis based on full knowledge of the system, pretest identification of potential vulnerabilities based on the pretest analysis, and testing designed to determine the exploitability of vulnerabilities. All parties agree to the rules of engagement before commencing penetration testing scenarios. Organizations correlate the rules of engagement for the penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries. Penetration testing may result in the exposure of information that is protected by laws or regulations, to individuals conducting the testing. Rules of engagement, contracts, or other appropriate mechanisms can be used to communicate expectations for how to protect this information. Risk assessments guide the decisions on the level of independence required for the personnel conducting penetration testing.

Related Controls RA-5, RA-10, SA-11, SR-5, SR-6.

JNCSF Alignment	JNCSF-190 Operation

Implementation Level 3

CA-8(1) Penetration Testing | Independent Penetration Testing Agent or Team

Control Context
Independent penetration testing agents or teams are individuals or groups who conduct impartial penetration testing of organizational systems. Impartiality implies that penetration testing agents or teams are free from perceived or actual conflicts of interest with respect to the development, operation, or management of the systems that are the targets of the penetration testing. CA-2(1) provides additional information on independent assessments that can be applied to penetration testing.

Related Controls	CA-2.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CA-8(2) Penetration Testing | Red Team Exercises

Control Context
Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of organizations and the capability to implement effective cyber defenses. Red team exercises simulate attempts by adversaries to compromise mission and business functions and provide a comprehensive assessment of the security and privacy posture of systems and organizations. Such attempts may include technology-based attacks and social engineering-based attacks. Technology-based attacks include interactions with hardware, software, or firmware components and/or mission and business processes. Social engineering-based attacks include interactions via email, telephone, shoulder surfing, or personal conversations. Red team exercises are most effective when conducted by penetration testing agents and teams with knowledge of and experience with current adversarial tactics, techniques, procedures, and tools. While penetration testing may be primarily laboratory-based testing, organizations can use red team exercises to provide more comprehensive assessments that reflect real-world conditions. The results from red team exercises can be used by organizations to improve security and privacy awareness and training and to assess control effectiveness.

Related Controls	None.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level I

CA-9 Internal System Connections

Control Context

Internal system connections are connections between organizational systems and separate constituent system components (i.e. connections between components that are part of the same system) including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

Related Controls AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12.

JNCSF Alignment JNCSF-31 Development, JNCSF-193 Operation

6 CONTROL FAMILY: CONFIGURATION MANAGEMENT

Implementation Level | I

CM-1 Policy and Procedures

Control Context
Configuration management policy and procedures address the controls in the CM 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 configuration management 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 that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to configuration management policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls
PM-9, PS-8, SA-8, SI-12.

JNCSF Alignment
Additional to Jordan's National Cybersecurity Framework

Implementation Level | I

CM-2 Baseline Configuration

Control Context
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 over time. Baseline configurations of systems reflect the current enterprise architecture.

Related Controls
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.

JNCSF Alignment
Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CM-2(2) Baseline Configuration | Automation Support for Accuracy and Currency

Control Context Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Automated tools can be used at the organization level, mission and business process level, or system level on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels. Automation support for accuracy and currency can be satisfied by the implementation of CM-8(2) for organizations that combine system component inventory and baseline configuration activities.

Related Controls CM-7, IA-3, RA-5.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CM-2(3) Baseline Configuration | Retention of Previous Configurations

Control Context Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, configuration records, and associated documentation.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CM-2(7) Baseline Configuration | Configure Systems and Components for High-risk Areas

Control Context When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the MP (Media Protection) family.

Related Controls	MP-4, MP-5.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CM-3 Configuration Change Control

Control Context	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, remediate 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.
Related Controls	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.
JNCSF Alignment	JNCSF-30 Development, JNCSF-33 Development, JNCSF-34 Development, JNCSF-63 Development, JNCSF-111 Delivery, JNCSF-114 Delivery, JNCSF-173 Operation

Implementation Level 3

CM-3(1) Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes

Control Context	None.
Related Controls	None.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CM-3(2) Configuration Change Control | Testing, Validation, and Documentation of Changes

Control Context	Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with system operations that support organizational mission and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures, system security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. Operational systems may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.
Related Controls	None.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CM-3(4) Configuration Change Control | Security and Privacy Representatives

Control Context	Information security and privacy representatives include system security officers, senior agency information security officers, senior agency officials for privacy, or system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change control element referred to in the second organization-defined parameter reflects the change control elements defined by organizations in CM-3g.
Related Controls	None.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CM-3(6) Configuration Change Control | Cryptography Management

Control Context	The controls referenced in the control enhancement refer to security and privacy controls from the control catalog. Regardless of the cryptographic mechanisms employed, processes and procedures are in place to manage those mechanisms. For example, if system components use certificates for identification and authentication, a process is implemented

to address the expiration of those certificates.

Related Controls SC-12.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

CM-4 Impact Analyses

Control Context Organizational personnel with security or privacy responsibilities conduct impact analyses. Individuals conducting impact analyses possess the necessary skills and technical expertise to analyze the changes to systems as well as the security or privacy ramifications. Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing the impact of changes on organizational supply chain partners with stakeholders; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses also include risk assessments to understand the impact of the changes and determine if additional controls are required.

Related Controls CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, RA-8, SA-5, SA-8, SA-10, SI-2.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CM-4(1) Impact Analyses | Separate Test Environments

Control Context A separate test environment requires an environment that is physically or logically separate and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment and that information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not implemented, organizations determine the strength of mechanism required when implementing logical separation.

Related Controls SA-11, SC-7.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CM-4(2) Impact Analyses | Verification of Controls

Control Context Implementation in this context refers to installing changed code in the operational system that may have an impact on security or privacy controls.

Related Controls SA-11, SC-3, SI-6.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

CM-5 Access Restrictions for Change

Control Context Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system can potentially have significant effects on the security of the systems or individuals' privacy. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes. Access restrictions include physical and logical access controls (see AC-3 and PE-3), software libraries, workflow automation, media libraries, abstract layers (i.e. changes implemented into external interfaces rather than directly into systems), and change windows (i.e. changes occur only during specified times).

Related Controls AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10.

JNCSF Alignment JNCSF-111 Delivery

Implementation Level 3

CM-5(1) Access Restrictions for Change | Automated Access Enforcement and Audit Records

Control Context Organizations log system accesses associated with applying configuration changes to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

Related Controls AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

CM-6 Configuration Settings

Control Context 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.

Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products and platforms as well as instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, government agencies, consortia, academia, industry, and other organizations in the public and private sectors.

Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency. Common secure configurations include the United States Government Configuration Baseline USGCB and security technical implementation guides (STIGs), which affect the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.

Related Controls 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.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CM-6(1) Configuration Settings | Automated Management, Application, and Verification

Control Context Automated tools (e.g. hardening tools, baseline configuration tools) can improve the accuracy, consistency, and availability of configuration settings information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

Related Controls CA-7.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CM-6(2) Configuration Settings | Respond to Unauthorized Changes

Control Context Responses to unauthorized changes to configuration settings include alerting designated organizational personnel, restoring established configuration settings, or—in extreme cases—halting affected system processing.

Related Controls IR-4, IR-6, SI-7.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

CM-7 Least Functionality

Control Context 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 over 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).

Related Controls 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.

JNCSF Alignment JNCSF-196 Operation

Implementation Level 2

CM-7(1) Least Functionality | Periodic Review

Control Context Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination. Such reviews are especially important during transition periods from older technologies to newer technologies (e.g. transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.

Related Controls AC-18.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CM-7(2) Least Functionality | Prevent Program Execution

Control Context Prevention of program execution addresses organizational policies, rules of behavior, and/or access agreements that restrict software usage and the terms and conditions imposed by the developer or manufacturer, including software licensing and copyrights. Restrictions include prohibiting auto-execute features, restricting roles allowed to approve program execution, permitting or prohibiting specific software programs, or restricting the number of program instances executed at the same time.

Related Controls CM-8, PL-4, PL-9, PM-5, PS-6.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CM-7(4) Least Functionality | Unauthorized Software — Deny-by-exception

Control Context 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.

Related Controls CM-6, CM-8, CM-10, PL-9, PM-5.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CM-7(5) Least Functionality | Authorized Software — Allow-by-exception

Control Context Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection for attacks that bypass application level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. The concept of permitting the execution of authorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. Organizations consider verifying the integrity of authorized software programs using digital signatures, cryptographic checksums, or hash functions. Verification of authorized software can occur either prior to execution or at system startup. The identification of authorized URLs for websites is addressed in CA-3(5) and SC-7.

Related Controls	CM-2, CM-6, CM-8, CM-10, PL-9, PM-5, SA-10, SC-34, SI-7.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

CM-8 System Component Inventory

Control Context

System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g. IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

Preventing duplicate accounting of system components addresses the lack of accountability that occurs when component ownership and system association is not known, especially in large or complex connected systems. Effective prevention of duplicate accounting of system components necessitates use of a unique identifier for each component. For software inventory, centrally managed software that is accessed via other systems is addressed as a component of the system on which it is installed and managed. Software installed on multiple organizational systems and managed at the system level is addressed for each individual system and may appear more than once in a centralized component inventory, necessitating a system association for each software instance in the centralized inventory to avoid duplicate accounting of components. Scanning systems implementing multiple network protocols (e.g. IPv4 and IPv6) can result in duplicate components being identified in different address spaces. The implementation of CM-8(7) can help to eliminate duplicate accounting of components.

Related Controls	CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PL-9, PM-5, SA-4, SA-5, SI-2, SR-4.
JNCSF Alignment	JNCSF-7 Security in Architecture and Portfolio, JNCSF-8 Security in Architecture and Portfolio

Implementation Level 2

CM-8(1) System Component Inventory | Updates During Installation and Removal

Control Context

Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented. System updates include hardware, software, and firmware components.

Related Controls PM-16.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CM-8(2) System Component Inventory | Automated Maintenance

Control Context Organizations maintain system inventories to the extent feasible. For example, virtual machines can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. Automated maintenance can be achieved by the implementation of CM-2(2) for organizations that combine system component inventory and baseline configuration activities.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CM-8(3) System Component Inventory | Automated Unauthorized Component Detection

Control Context Automated unauthorized component detection is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms may also be used to prevent the connection of unauthorized components (see CM-7(9)). Automated mechanisms can be implemented in systems or in separate system components. When acquiring and implementing automated mechanisms, organizations consider whether such mechanisms depend on the ability of the system component to support an agent or supplicant in order to be detected since some types of components do not have or cannot support agents (e.g. IoT devices, sensors). Isolation can be achieved , for example, by placing unauthorized system components in separate domains or subnets or quarantining such components. This type of component isolation is commonly referred to as sandboxing.

Related Controls AC-19, CA-7, RA-5, SC-3, SC-39, SC-44, SI-3, SI-4, SI-7.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CM-8(4) System Component Inventory | Accountability Information

Control Context Identifying individuals who are responsible and accountable for administering system components ensures that the assigned components are properly administered and that organizations can contact those individuals if some action is required (e.g. when the component is determined to be the source of a breach, needs to be recalled or replaced, or needs to be relocated).

Related Controls AC-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CM-9 Configuration Management Plan

Control Context Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g. the control of code and software libraries) and operational configuration management activities (e.g. control of installed components and how the components are configured). Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities.

Configuration management plans are generated during the development and acquisition stage of the system development life cycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents.

Organizations can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the organization with subsets of the plan implemented on a system by system basis. Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be configuration-managed. As systems continue through the system development life cycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.

Related Controls CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, RA-8, SA-10, SI-12.

JNCSF Alignment JNCSF-37 Development, JNCSF-38 Development

Implementation Level 1

CM-10 Software Usage Restrictions

Control Context
Software license tracking can be accomplished by manual or automated methods, depending on organizational needs. Examples of contract agreements include software license agreements and non-disclosure agreements.

Related Controls
AC-17, AU-6, CM-7, CM-8, PM-30, SC-7.

JNCSF Alignment
JNCSF-197 Operation, JNCSF-198 Operation

Implementation Level 1

CM-11 User-installed Software

Control Context
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.

Related Controls
AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7.

JNCSF Alignment
JNCSF-39 Development, JNCSF-199 Operation

Implementation Level 2

CM-12 Information Location

Control Context
Information location addresses the need to understand where information is being processed and stored. Information location includes identifying where specific information types and information reside in system components and how information is being processed so that information flow can be understood and adequate protection and policy management provided for such information and system components. The security category of the information is also a factor in determining the controls necessary to protect the information and the system component where the information resides (see FIPS 199). The location of the information and system components is also a factor in the architecture and design of the system (see SA-4, SA-8, SA-17).

Related Controls
AC-2, AC-3, AC-4, AC-6, AC-23, CM-8, PM-5, RA-2, SA-4, SA-8, SA-17, SC-4, SC-16, SC-28, SI-4, SI-7.

JNCSF Alignment
Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CM-12(1) Information Location | Automated Tools to Support Information Location

Control Context	The use of automated tools helps to increase the effectiveness and efficiency of the information location capability implemented within the system. Automation also helps organizations manage the data produced during information location activities and share such information across the organization. The output of automated information location tools can be used to guide and inform system architecture and design decisions.
Related Controls	None.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

7 CONTROL FAMILY: CONTINGENCY PLANNING

Implementation Level 1

CP-1 Policy and Procedures

Control Context

Contingency planning policy and procedures address the controls in the CP 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 contingency planning 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 that reflect 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to contingency planning policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls

PM-9, PS-8, SI-12.

JNCSF Alignment

JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level 1

CP-2 Contingency Plan

Control Context

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.

Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Organizations consider whether continuity of operations during an incident conflicts with the capability to automatically disable the system, as specified in IR-4(5). Incident response planning is part of contingency planning for organizations and is addressed in the IR (Incident Response) family.

Related Controls 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.

JNCSF Alignment JNCSF-202 Operation, JNCSF-206 Operation, JNCSF-205 Operation, JNCSF-208 Operation, JNCSF-210 Operation, JNCSF-212 Operation, JNCSF-213 Operation, JNCSF-214 Operation, JNCSF-217 Operation

Implementation Level 2

CP-2(1) Contingency Plan | Coordinate with Related Plans

Control Context Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and Occupant Emergency Plans.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CP-2(2) Contingency Plan | Capacity Planning

Control Context Capacity planning is needed because different threats can result in a reduction of the available processing, telecommunications, and support services intended to support essential mission and business functions. Organizations anticipate degraded operations during contingency operations and factor the degradation into capacity planning. For capacity planning, environmental support refers to any environmental factor for which the organization determines that it needs to provide support in a contingency situation, even if in a degraded state. Such determinations are based on an organizational assessment of risk, system categorization (impact level), and organizational risk tolerance.

Related Controls PE-11, PE-12, PE-13, PE-14, PE-18, SC-5.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CP-2(3) Contingency Plan | Resume Mission and Business Functions

Control Context Organizations may choose to conduct contingency planning activities to resume mission and business functions as part of business continuity planning or as part of business impact analyses. Organizations prioritize the resumption of mission and business functions. The time period for resuming mission and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CP-2(5) Contingency Plan | Continue Mission and Business Functions

Control Context Organizations may choose to conduct the contingency planning activities to continue mission and business functions as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CP-2(8) Contingency Plan | Identify Critical Assets

Control Context Organizations may choose to identify critical assets as part of criticality analysis, business continuity planning, or business impact analyses. Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include technical and operational aspects. Technical aspects include system components, information technology services, information technology products, and mechanisms. Operational aspects include procedures (i.e. manually executed operations) and personnel (i.e. individuals operating technical controls and/or executing manual procedures). Organizational program protection plans can assist in identifying critical assets. If critical assets are resident within or supported by external service providers, organizations consider implementing CP-2(7) as a control enhancement.

Related Controls CM-8, RA-9.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

CP-3 Contingency Training

Control Context Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and organizational officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Events that may precipitate an update to contingency training content include, but are not limited to, contingency plan testing or an actual contingency (lessons learned), assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. At the discretion of the organization, participation in a contingency plan test or exercise, including lessons learned sessions subsequent to the test or exercise, may satisfy contingency plan training requirements.

Related Controls AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.

JNCSF Alignment JNCSF-473 Foundational

Implementation Level 3

CP-3(1) Contingency Training | Simulated Events

Control Context The use of simulated events creates an environment for personnel to experience actual threat events, including cyber-attacks that disable websites, ransomware attacks that encrypt organizational data on servers, hurricanes that damage or destroy organizational facilities, or hardware or software failures.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

CP-4 Contingency Plan Testing

Control Context	Methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.
Related Controls	AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2.
JNCSF Alignment	JNCSF-41 Development

Implementation Level 2

CP-4(1) Contingency Plan Testing | Coordinate with Related Plans

Control Context	Plans related to contingency planning for organizational systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. However, it does require that if such organizational elements are responsible for related plans, organizations coordinate with those elements.
Related Controls	IR-8, PM-8.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CP-4(2) Contingency Plan Testing | Alternate Processing Site

Control Context	Conditions at the alternate processing site may be significantly different than the conditions at the primary site. Having the opportunity to visit the alternate site and experience the actual capabilities available at the site can provide valuable information on potential vulnerabilities that could affect essential organizational mission and business functions. The on-site visit can also provide an opportunity to refine the contingency plan to address the vulnerabilities discovered during testing.
Related Controls	CP-7.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CP-6 Alternate Storage Site

Control Context

Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

Related Controls CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.

JNCSF Alignment JNCSF-218 Operation, JNCSF-219 Operation

Implementation Level 2

CP-6(1) Alternate Storage Site | Separation from Primary Site

Control Context

Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls RA-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CP-6(2) Alternate Storage Site | Recovery Time and Recovery Point Objectives

Control Context

Organizations establish recovery time and recovery point objectives as part of contingency planning. Configuration of the alternate storage site includes physical facilities and the systems supporting recovery operations that ensure accessibility and correct execution.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CP-6(3) Alternate Storage Site | Accessibility

Control Context Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

Related Controls RA-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CP-7 Alternate Processing Site

Control Context Alternate processing sites are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as failover to a cloud-based service provider or other internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential mission and business functions despite disruption, compromise, or failure in organizational systems.

Related Controls CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CP-7(1) Alternate Processing Site | Separation from Primary Site

Control Context Threats that affect alternate processing sites are defined in organizational assessments of risk and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls RA-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CP-7(2) Alternate Processing Site | Accessibility

Control Context Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

Related Controls RA-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CP-7(3) Alternate Processing Site | Priority of Service

Control Context Priority of service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site. Organizations establish recovery time objectives as part of contingency planning.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CP-7(4) Alternate Processing Site | Preparation for Use

Control Context Site preparation includes establishing configuration settings for systems at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and logistical considerations are in place.

Related Controls CM-2, CM-6, CP-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CP-8 Telecommunications Services

Control Context

Telecommunications services (for data and voice) for primary and alternate processing and storage sites are in scope for CP-8. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential mission and business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines, network-based approaches to telecommunications, or the use of satellites. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

Related Controls CP-2, CP-6, CP-7, CP-11, SC-7.

JNCSF Alignment JNCSF-223 Operation

Implementation Level 2

CP-8(1) Telecommunications Services | Priority of Service Provisions

Control Context

Organizations consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority of service provisions.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CP-8(2) Telecommunications Services | Single Points of Failure

Control Context

In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is important to have provider transparency for the actual physical transmission capability for telecommunication services.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CP-8(3) Telecommunications Services | Separation of Primary and Alternate Providers

Control Context Threats that affect telecommunications services are defined in organizational assessments of risk and include natural disasters, structural failures, cyber or physical attacks, and errors of omission or commission. Organizations can reduce common susceptibilities by minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services that meet the separation needs addressed in the risk assessment.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CP-8(4) Telecommunications Services | Provider Contingency Plan

Control Context Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security and state and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

Related Controls CP-3, CP-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level I

CP-9 System Backup

Control Context 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.

Related Controls CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.

JNCSF Alignment JNCSF-225 Operation, JNCSF-226 Operation, JNCSF-227 Operation

Implementation Level 2

CP-9(1) System Backup | Testing for Reliability and Integrity

Control Context Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.

Related Controls CP-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CP-9(2) System Backup | Test Restoration Using Sampling

Control Context Organizations need assurance that system functions can be restored correctly and can support established organizational missions. To ensure that the selected system functions are thoroughly exercised during contingency plan testing, a sample of backup information is retrieved to determine whether the functions are operating as intended. Organizations can determine the sample size for the functions and backup information based on the level of assurance needed.

Related Controls CP-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CP-9(3) System Backup | Separate Storage for Critical Information

Control Context Separate storage for critical information applies to all critical information regardless of the type of backup storage media. Critical system software includes operating systems, middleware, cryptographic key management systems, and intrusion detection systems. Security-related information includes inventories of system hardware, software, and firmware components. Alternate storage sites, including geographically distributed architectures, serve as separate storage facilities for organizations. Organizations may provide separate storage by implementing automated backup processes at alternative storage sites (e.g. data centers).

Related Controls CM-2, CM-6, CM-8.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CP-9(5) System Backup | Transfer to Alternate Storage Site

Control Context System backup information can be transferred to alternate storage sites either electronically or by the physical shipment of storage media.

Related Controls CP-7, MP-3, MP-4, MP-5.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CP-9(8) System Backup | Cryptographic Protection

Control Context The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanisms selected is commensurate with the security category or classification of the information. Cryptographic protection applies to system backup information in storage at both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

Related Controls SC-12, SC-13, SC-28.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

CP-10 System Recovery and Reconstitution

Control Context 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.

Related Controls CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.

JNCSF Alignment JNCSF-229 Operation

Implementation Level 2

CP-10(2) System Recovery and Reconstitution | Transaction Recovery

Control Context Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

CP-10(4) System Recovery and Reconstitution | Restore Within Time Period

Control Context Restoration of system components includes reimaging, which restores the components to known, operational states.

Related Controls CM-2, CM-6.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

CP-10(6) System Recovery and Reconstitution | Component Protection

Control Context Protection of system recovery and reconstitution components (i.e. hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilers, and other system software.

Related Controls AC-3, AC-6, MP-2, MP-4, PE-3, PE-6.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | I |

CP-12 Safe Mode

Control Context For systems that support critical mission and business functions—including military operations, civilian space operations, nuclear power plant operations, and air traffic control operations (especially real-time operational environments)—organizations can identify certain conditions under which those systems revert to a predefined safe mode of operation. The safe mode of operation, which can be activated either automatically or manually, restricts the operations that systems can execute when those conditions are encountered. Restriction includes allowing only selected functions to execute that can be carried out under limited power or with reduced communications bandwidth.

Related Controls CM-2, SA-8, SC-24, SI-13, SI-17.

JNCSF Alignment JNCSF-231 Operation

8 CONTROL FAMILY: IDENTIFICATION AND AUTHENTICATION

Implementation Level 1

IA-1 Policy and Procedures

Control Context

Identification and authentication policy and procedures address the controls in the IA 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 identification and authentication 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 that reflect 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to identification and authentication policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls

AC-1, PM-9, PS-8, SI-12.

JNCSF Alignment

JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level 1

IA-2 Identification and Authentication (organizational Users)

Control Context

Organizations can satisfy the identification and authentication requirements by complying with the requirements in HSPD 12. Organizational users include employees or individuals who organizations consider to have an equivalent status to employees (e.g. contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.

Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities or, in the case of multi-factor authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where access is obtained through network connections (i.e. nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.

The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-8.

Related Controls	AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA-5, PE-2, PL-4, SA-4, SA-8.
JNCSF Alignment	JNCSF-116 Delivery

Implementation Level 1

IA-2(1) Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts

Control Context

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), or 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. 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 (i.e. local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Related Controls	AC-5, AC-6.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

IA-2(2) Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts

Control Context

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), or 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. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e. local, network, remote), non-privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Related Controls AC-5.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

IA-2(5) Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication

Control Context Individual authentication prior to shared group authentication mitigates the risk of using group accounts or authenticators.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

IA-2(6) Identification and Authentication (organizational Users) | Access to Accounts —separate Device

Control Context The purpose of requiring a device that is separate from the system to which the user is attempting to gain access for one of the factors during multi-factor authentication is to reduce the likelihood of compromising authenticators or credentials stored on the system. Adversaries may be able to compromise such authenticators or credentials and subsequently impersonate authorized users. Implementing one of the factors on a separate device (e.g. a hardware token), provides a greater strength of mechanism and an increased level of assurance in the authentication process.

Related Controls AC-6.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

IA-2(8) Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant

Control Context Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or cryptographic authenticators.

Related Controls	None.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

IA-3 Device Identification and Authentication

Control Context

Devices that require unique device-to-device identification and authentication are defined by type, device, or a combination of type and device. Organization-defined device types include devices that are not owned by the organization. Systems use shared known information (e.g. Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g. Institute of Electrical and Electronics Engineers (IEEE) 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Because of the challenges of implementing device authentication on a large scale, organizations can restrict the application of the control to a limited number/type of devices based on mission or business needs.

Related Controls	AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

IA-3(1) Device Identification and Authentication | Cryptographic Bidirectional Authentication

Control Context

A local connection is a connection with a device that communicates without the use of a network. A network connection is a connection with a device that communicates through a network. A remote connection is a connection with a device that communicates through an external network. Bidirectional authentication provides stronger protection to validate the identity of other devices for connections that are of greater risk.

Related Controls	SC-8, SC-12, SC-13.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

IA-3(4) Device Identification and Authentication | Device Attestation

Control Context Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. Device attestation can be determined via a cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the patches and updates are done securely and do not disrupt identification and authentication to other devices.

Related Controls CM-2, CM-3, CM-6.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

IA-4 Identifier Management

Control Context Common device identifiers include Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, or device-unique token identifiers. The management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices.

Related Controls AC-5, IA-2, IA-3, IA-5, IA-8, IA-9, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS-3, PS-4, PS-5, SC-37.

JNCSF Alignment JNCSF-44 Development, JNCSF-117 Delivery, JNCSF-118 Delivery, JNCSF-235 Operation

Implementation Level 2

IA-4(4) Identifier Management | Identify User Status

Control Context Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level I

IA-5 Authenticator Management

Control Context 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. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored in organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g. minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

Related Controls 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.

JNCSF Alignment JNCSF-45 Development, JNCSF-46 Development, JNCSF-119 Delivery, JNCSF-120 Delivery, JNCSF-121 Delivery, JNCSF-122 Delivery, JNCSF-237 Operation

Implementation Level I

IA-5(1) Authenticator Management | Password-based Authentication

Control Context 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.

Related Controls IA-6.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

IA-5(2) Authenticator Management | Public Key-based Authentication

Control Context Public key cryptography is a valid authentication mechanism for individuals, machines, and devices. For PKI solutions, status information for certification paths includes certificate revocation lists or certificate status protocol responses. For PIV cards, certificate validation involves the construction and verification of a certification path to the Common Policy Root trust anchor, which includes certificate policy processing. Implementing a local cache of revocation data to support path discovery and validation also supports system availability in situations where organizations are unable to access revocation information via the network.

Related Controls IA-3, SC-17.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

IA-5(6) Authenticator Management | Protection of Authenticators

Control Context For systems that contain multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems. Security categories of information are determined as part of the security categorization process.

Related Controls RA-2.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

IA-6 Authentication Feedback

Control Context Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems, such as mobile devices with small displays, the threat may be less significant and is balanced against the increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authentication feedback is selected accordingly. Obscuring authentication feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before obscuring it.

Related Controls AC-3.

JNCSF Alignment JNCSF-47 Development

Implementation Level 1

IA-7 Cryptographic Module Authentication

Control Context Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

Related Controls AC-3, IA-5, SA-4, SC-12, SC-13.

JNCSF Alignment JNCSF-48 Development

Implementation Level 1

IA-8 Identification and Authentication (non-organizational Users)

Control Context Non-organizational users include system users other than organizational users explicitly covered by IA-2. Non-organizational users are uniquely identified and authenticated for accesses other than those explicitly identified and documented in AC-14. Identification and authentication of non-organizational users accessing government systems may be required to protect government, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations consider many factors—including security, privacy, scalability, and practicality—when balancing the need to ensure ease of use for access to government information and systems with the need to protect and adequately mitigate risk.

Related Controls AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA-3, SA-4, SC-8.

JNCSF Alignment JNCSF-49 Development

Implementation Level 3

IA-8(2) Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators

Control Context Acceptance of only NIST or Government compliant external authenticators applies to organizational systems that are accessible to the public (e.g. public-facing websites). Approved external authenticators meet or exceed the minimum Government-wide technical, security, privacy, and organizational maturity requirements. Meeting or exceeding requirements allows Government relying parties to trust external authenticators in connection with an authentication transaction at a specified authenticator assurance level.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

IA-8(4) Identification and Authentication (non-organizational Users) | Use of Defined Profiles

Control Context Organizations define profiles for identity management based on open identity management standards. To ensure that open identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the Government assesses and scopes the standards and technology implementations against applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

IA-9 Service Identification and Authentication

Control Context Services that may require identification and authentication include web applications using digital certificates or services or applications that query a database. Identification and authentication methods for system services and applications include information or code signing, provenance graphs, and electronic signatures that indicate the sources of services. Decisions regarding the validity of identification and authentication claims can be made by services separate from the services acting on those decisions. This can occur in distributed system architectures. In such situations, the identification and authentication decisions (instead of actual identifiers and authentication data) are provided to the services that need to act on those decisions.

Related Controls IA-3, IA-4, IA-5, SC-8.

JNCSF Alignment JNCSF-123 - Delivery

Implementation Level | 1

IA-11 Re-authentication

Control Context: In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically.

Related Controls: AC-3, AC-11, IA-2, IA-3, IA-4, IA-8.

JNCSF Alignment: JNCSF-26 Development

Implementation Level | 2

IA-12 Identity Proofing

Control Context: Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts. Standards and guidelines specifying identity assurance levels for identity proofing include SP 800-63-3 and SP 800-63A. Organizations may be subject to laws, executive orders, directives, regulations, or policies that address the collection of identity evidence. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: AC-5, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8.

JNCSF Alignment: Additional to Jordan's National Cybersecurity Framework

Implementation Level | 3

IA-12(1) Identity Proofing | Supervisor Authorization

Control Context: Including supervisor or sponsor authorization as part of the registration process provides an additional level of scrutiny to ensure that the user's management chain is aware of the account, the account is essential to carry out organizational missions and functions, and the user's privileges are appropriate for the anticipated responsibilities and authorities within the organization.

Related Controls: None.

JNCSF Alignment: Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

IA-12(2) Identity Proofing | Identity Evidence

Control Context Identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity or at least increases the work factor of potential adversaries. The forms of acceptable evidence are consistent with the risks to the systems, roles, and privileges associated with the user’s account.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

IA-12(3) Identity Proofing | Identity Evidence Validation and Verification

Control Context Validation and verification of identity evidence increases the assurance that accounts and identifiers are being established for the correct user and authenticators are being bound to that user. Validation refers to the process of confirming that the evidence is genuine and authentic, and the data contained in the evidence is correct, current, and related to an individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risks to the systems, roles, and privileges associated with the users account.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

IA-12(4) Identity Proofing | In-person Validation and Verification

Control Context In-person proofing reduces the likelihood of fraudulent credentials being issued because it requires the physical presence of individuals, the presentation of physical identity documents, and actual face-to-face interactions with designated registration authorities.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

IA-12(5) Identity Proofing | Address Confirmation

Control Context	To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, organizations can use out-of-band methods to ensure that the individual associated with an address of record is the same individual that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts is obtained from records and not self-asserted by the user. The address can include a physical or digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.
Related Controls	IA-12.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

9 CONTROL FAMILY: INCIDENT RESPONSE

Implementation Level I

IR-1 Policy and Procedures

Control Context

Incident response policy and procedures address the controls in the IR 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 incident response 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 that reflect 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to incident response policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls PM-9, PS-8, SI-12.

JNCSF Alignment JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational

Implementation Level I

IR-2 Incident Response Training

Control Context

Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of AT-2 or AT-3. Events that may precipitate an update to incident response training content include, but are not limited to, incident response plan testing or response to an actual incident (lessons learned), assessment or audit findings, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls AT-2, AT-3, AT-4, CP-3, IR-3, IR-4, IR-8, IR-9.

JNCSF Alignment JNCSF-249 Operation

Implementation Level 3

IR-2(1) Incident Response Training | Simulated Events

Control Context Organizations establish requirements for responding to incidents in incident response plans. Incorporating simulated events into incident response training helps to ensure that personnel understand their individual responsibilities and what specific actions to take in crisis situations.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

IR-2(2) Incident Response Training | Automated Training Environments

Control Context Automated mechanisms can provide a more thorough and realistic incident response training environment. This can be accomplished, for example, by providing more complete coverage of incident response issues, selecting more realistic training scenarios and environments, and stressing the response capability.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level I

IR-2(3) Incident Response Training | Breach

Control Context For government agencies, an incident that involves personally identifiable information is considered a breach. A breach results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes. The incident response training emphasizes the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, oral, and electronic. Incident response training includes tabletop exercises that simulate a breach. See IR-2(1).

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

IR-3 Incident Response Testing

Control Context Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

Related Controls CP-3, CP-4, IR-2, IR-4, IR-8, PM-14.

JNCSF Alignment JNCSF-250 Operation

Implementation Level 2

IR-3(2) Incident Response Testing | Coordination with Related Plans

Control Context Organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

IR-4 Incident Handling

Control Context Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations consider incident response as part of the definition, design, and development of mission and business processes and systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring; user or administrator reports; and reported supply chain events. An effective incident handling capability includes coordination among many organizational entities (e.g. mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices). Suspected security incidents include the receipt of suspicious email communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components. For CNI operators and government entities, an incident that involves personally identifiable information is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes.

Related Controls AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.

JNCSF Alignment JNCSF-213 Operation, JNCSF-252 Operation, JNCSF-255 Operation

Implementation Level 2

IR-4(1) Incident Handling | Automated Incident Handling Processes

Control Context Automated mechanisms that support incident handling processes include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

IR-4(4) Incident Handling | Information Correlation

Control Context Sometimes, a threat event, such as a hostile cyber-attack, can only be observed by bringing together information from different sources, including various reports and reporting procedures established by organizations.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

IR-4(11) Incident Handling | Integrated Incident Response Team

Control Context An integrated incident response team is a team of experts that assesses, documents, and responds to incidents so that organizational systems and networks can recover quickly and implement the necessary controls to avoid future incidents. Incident response team personnel include forensic and malicious code analysts, tool developers, systems security and privacy engineers, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions. For some organizations, the incident response team can be a cross-organizational entity.

An integrated incident response team facilitates information sharing and allows organizational personnel (e.g. developers, implementers, and operators) to leverage team knowledge of the threat and implement defensive measures that enable organizations to deter intrusions more effectively. Moreover, integrated teams promote the rapid detection of intrusions, the development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing cyber intelligence development. Integrated incident response teams are better able to identify adversary tactics, techniques, and procedures that are linked to the operations tempo or specific mission and business functions and to define responsive actions in a way that does not disrupt those mission and business functions. Incident response teams can be distributed within organizations to make the capability resilient.

Related Controls AT-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

IR-5 Incident Monitoring

Control Context Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. IR-4 provides information on the types of incidents that are appropriate for monitoring.

Related Controls AU-6, AU-7, IR-4, IR-6, IR-8, PE-6, PM-5, SC-5, SC-7, SI-3, SI-4, SI-7.

JNCSF Alignment JNCSF-256 Operation

Implementation Level 3

IR-5(1) Incident Monitoring | Automated Tracking, Data Collection, and Analysis

Control Context Automated mechanisms for tracking incidents and collecting and analyzing incident information include Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

IR-6 Incident Reporting

Control Context The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Incident information can inform risk assessments, control effectiveness assessments, security requirements for acquisitions, and selection criteria for technology products.

Related Controls CM-6, CP-2, IR-4, IR-5, IR-8, IR-9.

JNCSF Alignment JNCSF-257 Operation, JNCSF-258 Operation

Implementation Level 2

IR-6(1) Incident Reporting | Automated Reporting

Control Context The recipients of incident reports are specified in IR-6b. Automated reporting mechanisms include email, posting on websites (with automatic updates), and automated incident response tools and programs.

Related Controls IR-7.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

IR-6(3) Incident Reporting | Supply Chain Coordination

Control Context Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include compromises or breaches that involve information technology products, system components, development processes or personnel, distribution processes, or warehousing facilities. Organizations determine the appropriate information to share and consider the value gained from informing external organizations about supply chain incidents, including the ability to improve processes or to identify the root cause of an incident.

Related Controls SR-8.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | 1

IR-7 Incident Response Assistance

Control Context: Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensics services or consumer redress services, when required.

Related Controls: AT-2, AT-3, IR-4, IR-6, IR-8, PM-22, PM-26, SA-9, SI-18.

JNCSF Alignment: Additional to Jordan's National Cybersecurity Framework

Implementation Level | 2

IR-7(1) Incident Response Assistance | Automation Support for Availability of Information and Support

Control Context: Automated mechanisms can provide a push or pull capability for users to obtain incident response assistance. For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

Related Controls: None.

JNCSF Alignment: Additional to Jordan's National Cybersecurity Framework

Implementation Level | 1

IR-8 Incident Response Plan

Control Context: It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information (i.e. breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

Related Controls: AC-2, CP-2, CP-4, IR-4, IR-7, IR-9, PE-6, PL-2, SA-15, SI-12, SR-8.

JNCSF Alignment: JNCSF-208 Operation, JNCSF-210 Operation, JNCSF-212 Operation, JNCSF-214 Operation, JNCSF-217 Operation, JNCSF-260 Operation, JNCSF-261 Operation, JNCSF-262 Operation, JNCSF-263 Operation, JNCSF-264 Operation, JNCSF-265 Operation, JNCSF-266 Operation

10 CONTROL FAMILY: MAINTENANCE

Implementation Level I

MA-1 Policy and Procedures

Control Context Maintenance policy and procedures address the controls in the MA 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 maintenance 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 that reflect 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to maintenance policy and procedures assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls PM-9, PS-8, SI-12.

JNCSF Alignment JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level I

MA-2 Controlled Maintenance

Control Context Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations consider supply chain-related risks associated with replacement components for systems.

Related Controls CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-4, SR-11.

JNCSF Alignment JNCSF-273 Operation, JNCSF-274 Operation, JNCSF-275 Operation, JNCSF-276 Operation, JNCSF-277 Operation, JNCSF-278 Operation

Implementation Level 3

MA-2(2) Controlled Maintenance | Automated Maintenance Activities

Optional

Control Context The use of automated mechanisms to manage and control system maintenance programs and activities helps to ensure the generation of timely, accurate, complete, and consistent maintenance records.

Related Controls MA-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

MA-3 Maintenance Tools

Control Context Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for the approval of maintenance tools and how that approval is documented. A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers. The hardware and software components that support maintenance and are a part of the system (including the software implementing utilities such as ping, ls, ipconfig, or the hardware and software implementing the monitoring port of an Ethernet switch) are not addressed by maintenance tools.

Related Controls MA-2, PE-16.

JNCSF Alignment JNCSF-11 Security in Architecture and Portfolio

Implementation Level 2

MA-3(1) Maintenance Tools | Inspect Tools

Control Context Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor’s website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

Related Controls SI-7.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

MA-3(2) Maintenance Tools | Inspect Media

Control Context If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations determine that the media contains malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

Related Controls SI-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

MA-3(3) Maintenance Tools | Prevent Unauthorized Removal

Control Context Organizational information includes all information owned by organizations and any information provided to organizations for which the organizations serve as information stewards.

Related Controls MP-6.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

MA-4 Nonlocal Maintenance

Control Context Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Authentication techniques used to establish nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Strong authentication requires authenticators that are resistant to replay attacks and employ multi-factor authentication. Strong authenticators include PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished, in part, by other controls. SP 800-63B provides additional guidance on strong authentication and authenticators.

Related Controls AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL-2, SC-7, SC-10.

JNCSF Alignment JNCSF-279 Operation, JNCSF-280 Operation, JNCSF-281 Operation, JNCSF-283 Operation

Implementation Level 2

MA-4(1) Nonlocal Maintenance | Logging and Review

Control Context Audit logging for nonlocal maintenance is enforced by AU-2. Audit events are defined in AU-2a.

Related Controls AU-6, AU-12.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

MA-4(3) Nonlocal Maintenance | Comparable Security and Sanitization

Control Context Comparable security capability on systems, diagnostic tools, and equipment providing maintenance services implies that the implemented controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.

Related Controls MP-6, SI-3, SI-7.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

MA-5 Maintenance Personnel

Control Context Maintenance personnel refers to individuals who perform hardware or software maintenance on organizational systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems, while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel—such as information technology manufacturers, vendors, systems integrators, and consultants—may require privileged access to organizational systems, such as when they are required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Related Controls AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.

JNCSF Alignment JNCSF-125 Delivery, JNCSF-126 Delivery, JNCSF-127 Delivery

Implementation Level 3

MA-5(1) Maintenance Personnel | Individuals Without Appropriate Access

Control Context Procedures for individuals who lack appropriate security clearances or who are not U.S. citizens are intended to deny visual and electronic access to classified or controlled unclassified information contained on organizational systems. Procedures for the use of maintenance personnel can be documented in security plans for the systems.

Related Controls MP-6, PL-2.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

MA-6 Timely Maintenance

Optional

Control Context Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support include having appropriate contracts in place.

Related Controls CM-8, CP-2, CP-7, RA-7, SA-15, SI-13, SR-2, SR-3, SR-4.

JNCSF Alignment JNCSF-284 Operation

11 CONTROL FAMILY: MEDIA PROTECTION

Implementation Level | 1

MP-1 Policy and Procedures

Control Context Media protection policy and procedures address the controls in the MP 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 media protection 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 that reflect 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls PM-9, PS-8, SI-12.

JNCSF Alignment JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level | 1

MP-2 Media Access

Control Context System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g. solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media.

Related Controls AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SC-34, SI-12.

JNCSF Alignment JNCSF-285 Operation

Implementation Level 2

MP-3 Media Marking

Control Context

Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g. solid state, magnetic), flash drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Controlled unclassified information is defined by the Local law and regulator which should provide guidance on the appropriate safeguarding and dissemination requirements for such information. Security markings are generally not required for media that contains information determined by organizations to be in the public domain or to be publicly releasable. Some organizations may require markings for public information indicating that the information is publicly releasable. System media marking reflects applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls AC-16, CP-9, MP-5, PE-22, SI-12.

JNCSF Alignment JNCSF-286 Operation, JNCSF-287 Operation

Implementation Level 2

MP-4 Media Storage

Control Context

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g. solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on organizations, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

Related Controls AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SC-34, SI-12.

JNCSF Alignment JNCSF-477 Foundational, JNCSF-478 Foundational

Implementation Level 2

MP-5 Media Transport

Control Context

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g. solid state and magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of system media in accordance with organizational assessments of risk. Organizations maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records.

Related Controls

AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28, SC-34.

JNCSF Alignment

JNCSF-288 Operation, JNCSF-289 Operation, JNCSF-290 Operation, JNCSF-291 Operation

Implementation Level 1

MP-6 Media Sanitization

Control Context

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 use discretion on the employment of 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 from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media that contains classified information. NARA policies control the sanitization process for controlled unclassified information.

Related Controls AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11.

JNCSF Alignment JNCSF-292 Operation, JNCSF-479 Foundational

Implementation Level 3

MP-6(1) Media Sanitization | Review, Approve, Track, Document, and Verify

Control Context Organizations review and approve media to be sanitized to ensure compliance with records retention policies. Tracking and documenting actions include listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken and personnel who performed the verification, and the disposal actions taken. Organizations verify that the sanitization of the media was effective prior to disposal.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

MP-6(2) Media Sanitization | Equipment Testing

Control Context Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities, including government agencies or external service providers.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

MP-6(3) Media Sanitization | Nondestructive Techniques

Control Context Portable storage devices include external or removable hard disk drives (e.g. solid state, magnetic), optical discs, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks. Portable storage devices can be obtained from untrustworthy sources and contain malicious code that can be inserted into or transferred to organizational systems through USB ports or other entry portals. While scanning storage devices is recommended, sanitization provides additional assurance that such devices are free of malicious code. Organizations consider nondestructive sanitization of portable storage devices when the devices are purchased from manufacturers or vendors prior to initial use or when organizations cannot maintain a positive chain of custody for the devices.

Related Controls	None.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level | I

MP-7 Media Use

Control Context

System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, compact discs, digital versatile discs, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to MP-2, which restricts user access to media, MP-7 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations use technical and nontechnical controls to restrict the use of system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports or disabling or removing the ability to insert, read, or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices, including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, such as by prohibiting the use of writeable, portable storage devices and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for storage devices reduces the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices.

Related Controls	AC-19, AC-20, PL-4, PM-12, SC-34, SC-41.
JNCSF Alignment	JNCSF-293 Operation

12 CONTROL FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

Implementation Level 1

PE-2 Physical Access Authorizations

Control Context	Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include ID badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.
Related Controls	AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PM-12, PS-3, PS-4, PS-5, PS-6.
JNCSF Alignment	JNCSF-480 Foundational, JNCSF-481 Foundational, JNCSF-482 Foundational

Implementation Level 1

PE-2(1) Physical Access Authorizations | Access by Position or Role

Control Context	Role-based facility access includes access by authorized permanent and regular/routine maintenance personnel, duty officers, and emergency medical staff.
Related Controls	AC-2, AC-3, AC-6.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

PE-2(3) Physical Access Authorizations | Restrict Unescorted Access

Control Context	-
Related Controls	PS-2, PS-6.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

PE-3 Physical Access Control

Optional

Control Context

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.

Related Controls

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.

JNCSF Alignment

Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

PE-3(1) Physical Access Control | System Access

Optional

Control Context

Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.

Related Controls

None.

JNCSF Alignment

Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

PE-4 Access Control for Transmission

Control Context

Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.

Related Controls AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.

JNCSF Alignment JNCSF-488 Foundational

Implementation Level 2

PE-5 Access Control for Output Devices

Control Context Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

Related Controls PE-2, PE-3, PE-4, PE-18.

JNCSF Alignment JNCSF-489 Foundational

Implementation Level 1

PE-6 Monitoring Physical Access

Control Context 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.

Related Controls AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.

JNCSF Alignment JNCSF-297 Operation, JNCSF-484 Foundational, JNCSF-490 Foundational

Implementation Level 2

PE-6(1) *Optional* Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment

Control Context Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and security guards by triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

PE-6(4) Monitoring Physical Access | Monitoring Physical Access to Systems

Optional

Control Context Monitoring physical access to systems provides additional monitoring for those areas within facilities where there is a concentration of system components, including server rooms, media storage areas, and communications centers. Physical access monitoring can be coordinated with intrusion detection systems and system monitoring capabilities to provide comprehensive and integrated threat coverage for the organization.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

PE-8 Visitor Access Records

Control Context Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine if access authorizations are current and are still required to support organizational mission and business functions. Access records are not required for publicly accessible areas.

Related Controls PE-2, PE-3, PE-6.

JNCSF Alignment JNCSF-491 Foundational

Implementation Level 3

PE-8(1) Visitor Access Records | Automated Records Maintenance and Review

Control Context Visitor access records may be stored and maintained in a database management system that is accessible by organizational personnel. Automated access to such records facilitates record reviews on a regular basis to determine if access authorizations are current and still required to support organizational mission and business functions.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

PE-9 Power Equipment and Cabling

Optional

Control Context Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptable power sources in offices or data centers, generators and power cabling outside of buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.

Related Controls PE-4.

JNCSF Alignment JNCSF-492 Foundational

Implementation Level 2

PE-10 Emergency Shutoff

Optional

Control Context Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

Related Controls PE-15.

JNCSF Alignment JNCSF-493 Foundational, JNCSF-494 Foundational

Implementation Level 2

PE-11 Emergency Power

Optional

Control Context: An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from unanticipated power interruptions from the main power source by providing energy stored in batteries, supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or properly shut down the system.

Related Controls: AT-3, CP-2, CP-7.

JNCSF Alignment: JNCSF-495 Foundational

Implementation Level 3

PE-11(1) Emergency Power | Alternate Power Supply — Minimal Operational Capability

Control Context: Provision of an alternate power supply with minimal operating capability can be satisfied by accessing a secondary commercial power supply or other external power supply.

Related Controls: None.

JNCSF Alignment: Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

PE-12 Emergency Lighting

Optional

Control Context: 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.

Related Controls: CP-2, CP-7.

JNCSF Alignment: JNCSF-496 Foundational

Implementation Level | 1

PE-13 Fire Protection

Optional

Control Context 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.

Related Controls AT-3.

JNCSF Alignment JNCSF-497 Foundational

Implementation Level | 2

PE-13(1) Fire Protection | Detection Systems — Automatic Activation and Notification

Optional

Control Context Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g. to enter to facilities where access is restricted due to the classification or impact level of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | 3

PE-13(2) Fire Protection | Suppression Systems — Automatic Activation and Notification

Optional

Control Context Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances (e.g. to enter to facilities where access is restricted due to the impact level or classification of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

PE-14 Environmental Controls

Optional

Control Context The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g. data centers, mainframe computer rooms, and server rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organizational mission and business functions.

Related Controls AT-3, CP-2.

JNCSF Alignment JNCSF-498 Foundational

Implementation Level 1

PE-15 Water Damage Protection

Optional

Control Context The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.

Related Controls AT-3, PE-10.

JNCSF Alignment JNCSF-499 Foundational

Implementation Level 3

PE-15(1) Water Damage Protection | Automation Support

Optional

Control Context Automated mechanisms include notification systems, water detection sensors, and alarms.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

PE-16 Delivery and Removal

Control Context Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.

Related Controls CM-3, CM-8, MA-2, MA-3, MP-5, PE-20, SR-2, SR-3, SR-4, SR-6.

JNCSF Alignment JNCSF-500 Foundational

Implementation Level 2

PE-17 Alternate Work Site

Control Context Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

Related Controls AC-17, AC-18, CP-7.

JNCSF Alignment JNCSF-298 Operation, JNCSF-501 Foundational, JNCSF-502 Foundational

Implementation Level 3

PE-18 Location of System Components

Optional

Control Context Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Organizations consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to organizational communications using wireless packet sniffers or microphones, or unauthorized disclosure of information.

Related Controls CP-2, PE-5, PE-19, PE-20, RA-3.

JNCSF Alignment JNCSF-299 Operation

Implementation Level 3

PE-20 Asset Monitoring and Tracking

Optional

Control Context	Asset location technologies can help ensure that critical assets—including vehicles, equipment, and system components—remain in authorized locations. Organizations consult with the Office of the General Counsel and senior agency official for privacy regarding the deployment and use of asset location technologies to address potential privacy concerns.
Related Controls	CM-8, PE-16, PM-8.
JNCSF Alignment	JNCSF-300 Operation

13 CONTROL FAMILY: PLANNING

Implementation Level | 1

PL-1 Policy and Procedures

Control Context

Planning policy and procedures for the controls in the PL family 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 their development. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission level 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 that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to planning policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls

PM-9, PS-8, SI-12.

JNCSF Alignment

JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level | 1

PL-2 System Security and Privacy Plans

Control Context

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). Section 2.1 describes the different types of requirements that are relevant to organizations during the system development life cycle and the relationship between requirements and controls.

Organizations may develop a single, integrated security and privacy plan or maintain separate plans. Security and privacy plans relate security and privacy requirements to a set of controls and control enhancements. The plans describe how the controls and control enhancements meet the security and privacy requirements but do not provide detailed, technical descriptions of the design or implementation of the controls and control enhancements. Security and privacy plans contain sufficient information (including specifications of control parameter values for selection and assignment operations explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented.

Security and privacy plans need not be single documents. The plans can be a collection of various documents, including documents that already exist. Effective security and privacy plans make extensive use of references to policies, procedures, and additional documents, including design and implementation specifications where more detailed information can be obtained. The use of references helps reduce the documentation associated with security and privacy programs and maintains the security- and privacy-related information in other established management and operational areas, including enterprise architecture, system development life cycle, systems engineering, and acquisition. Security and privacy plans need not contain detailed contingency plan or incident response plan information but can instead provide—explicitly or by reference—sufficient information to define what needs to be accomplished by those plans.

Security- and privacy-related activities that may require coordination and planning with other individuals or groups within the organization include assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing. Planning and coordination include emergency and nonemergency (i.e. planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security- and privacy-related activities can also be included in other documents, as appropriate.

Related Controls 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.

JNCSF Alignment JNCSF-9 Security in Architecture and Portfolio, JNCSF-12 Security in Architecture and Portfolio, JNCSF-13 Security in Architecture and Portfolio, JNCSF-209 Operation, JNCSF-211 Operation, JNCSF-215 Operation, JNCSF-216 Operation

Implementation Level 1

PL-4 Rules of Behavior

Control Context Rules of behavior represent a type of access agreement for organizational users. Other types of access agreements include nondisclosure agreements, conflict-of-interest agreements, and acceptable use agreements (see PS-6). Organizations consider rules of behavior based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users, including individuals who receive information from federal systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for organizational and non-organizational users can also be established in AC-8. The related controls section provides a list of controls that are relevant to organizational rules of behavior. PL-4b, the documented acknowledgment portion of the control, may be satisfied by the literacy training and awareness and role-based training programs conducted by organizations if such training includes rules of behavior. Documented acknowledgements for rules of behavior include electronic or physical signatures and electronic agreement check boxes or radio buttons.

Related Controls AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, SI-12.

JNCSF Alignment JNCSF-507 Foundational, JNCSF-509 Foundational, JNCSF-510 Foundational

Implementation Level 2

PL-4(1) Rules of Behavior | Social Media and External Site/application Usage Restrictions

Control Context Social media, social networking, and external site/application usage restrictions address rules of behavior related to the use of social media, social networking, and external sites when organizational personnel are using such sites for official duties or in the conduct of official business, when organizational information is involved in social media and social networking transactions, and when personnel access social media and networking sites from organizational systems. Organizations also address specific rules that prevent unauthorized entities from obtaining non-public organizational information from social media and networking sites either directly or through inference. Non-public information includes personally identifiable information and system account information.

Related Controls AC-22, AU-13.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

PL-8 Security and Privacy Architectures

Control Context The security and privacy architectures at the system level are consistent with the organization-wide security and privacy architectures described in PM-7, which are integral to and developed as part of the enterprise architecture. The architectures include an architectural description, the allocation of security and privacy functionality (including controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The architectures can also include other information, such as user roles and the access privileges assigned to each role; security and privacy requirements; types of information processed, stored, and transmitted by the system; supply chain risk management requirements; restoration priorities of information and system services; and other protection needs.

SP 800-160-1 provides guidance on the use of security architectures as part of the system development life cycle process. OMB M-19-03 requires the use of the systems security engineering concepts described in SP 800-160-1 for high value assets. Security and privacy architectures are reviewed and updated throughout the system development life cycle, from analysis of alternatives through review of the proposed architecture in the RFP responses to the design reviews before and during implementation (e.g. during preliminary design reviews and critical design reviews).

In today's modern computing architectures, it is becoming less common for organizations to control all information resources. There may be key dependencies on external information services and service providers. Describing such dependencies in the security and privacy architectures is necessary for developing a comprehensive mission and business protection strategy. Establishing, developing, documenting, and maintaining under configuration control a baseline configuration for organizational systems is critical to implementing and maintaining effective architectures. The development of the architectures is coordinated with the senior agency information security officer and the senior agency official for privacy to ensure that the controls needed to support security and privacy requirements are identified and effectively implemented. In many circumstances, there may be no distinction between the security and privacy architecture for a system. In other circumstances, security objectives may be adequately satisfied, but privacy objectives may only be partially satisfied by the security requirements. In these cases, consideration of the privacy requirements needed to achieve satisfaction will result in a distinct privacy architecture. The documentation, however, may simply reflect the combined architectures.

PL-8 is primarily directed at organizations to ensure that architectures are developed for the system and, moreover, that the architectures are integrated with or tightly coupled to the enterprise architecture. In contrast, SA-17 is primarily directed at the external information technology product and system developers and integrators. SA-17, which is complementary to PL-8, is selected when organizations outsource the development of systems or components to external entities and when there is a need to demonstrate consistency with the organization's enterprise architecture and security and privacy architectures.

Related Controls CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17, SC-7.

JNCSF Alignment JNCSF-14 Security in Architecture and Portfolio, JNCSF-15 Security in Architecture and Portfolio, JNCSF-16 Security in Architecture and Portfolio, JNCSF-17 Security in Architecture and Portfolio

Implementation Level 2

PL-8(1) Security and Privacy Architectures | Defense in Depth

Control Context Organizations strategically allocate security and privacy controls in the security and privacy architectures so that adversaries must overcome multiple controls to achieve their objective. Requiring adversaries to defeat multiple controls makes it more difficult to attack information resources by increasing the work factor of the adversary; it also increases the likelihood of detection. The coordination of allocated controls is essential to ensure that an attack that involves one control does not create adverse, unintended consequences by interfering with other controls. Unintended consequences can include system lockout and cascading alarms. The placement of controls in systems and organizations is an important activity that requires thoughtful analysis. The value of organizational assets is an important consideration in providing additional layering. Defense-in-depth architectural approaches include modularity and layering (see SA-8(3)), separation of system and user functionality (see SC-2), and security function isolation (see SC-3).

Related Controls SC-2, SC-3, SC-29, SC-36.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level |

	I

PL-10 Baseline Selection

Control Context — Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (see PL-11).

Related Controls — PL-2, PL-11, RA-2, RA-3, SA-8.

JNCSF Alignment — Additional to Jordan's National Cybersecurity Framework

Implementation Level

	I

PL-11 Baseline Tailoring

Control Context — The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success.

Related Controls — PL-10, RA-2, RA-3, RA-9, SA-8.

JNCSF Alignment — Additional to Jordan's National Cybersecurity Framework

14 CONTROL FAMILY: RISK ASSESSMENT

Implementation Level | 1

RA-1 Policy and Procedures

Control Context

Risk assessment policy and procedures address the controls in the RA 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 risk assessment 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to risk assessment policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls

PM-9, PS-8, SI-12.

JNCSF Alignment

JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level | 1

RA-2 Security Categorization

Control Context

Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in systems security engineering processes that is carried out throughout the system development life cycle. Organizations can use privacy risk assessments or privacy impact assessments to better understand the potential adverse effects on individuals. CNSSI 1253 provides additional guidance on categorization for national security systems.

Organizations conduct the security categorization process as an organization-wide activity with the direct involvement of chief information officers, senior agency information security officers, senior agency officials for privacy, system owners, mission and business owners, and information owners or stewards. Organizations consider the potential adverse impacts to other organizations and, in accordance with USA PATRIOT and Homeland Security Presidential Directives, potential national-level adverse impacts.

Security categorization processes facilitate the development of inventories of information assets and, along with CM-8, mappings to specific system components where information is processed, stored, or transmitted. The security categorization process is revisited throughout the system development life cycle to ensure that the security categories remain accurate and relevant.

Related Controls CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SA-8, SC-7, SC-38, SI-12.

JNCSF Alignment JNCSF-133 Delivery, JNCSF-536 Foundational, JNCSF-537 Foundational

Implementation Level I

RA-3 Risk Assessment

Control Context Risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation. Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.

Organizations can conduct risk assessments at all three levels in the risk management hierarchy (i.e. organization level, mission/business process level, or information system level) and at any stage in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including preparation, categorization, control selection, control implementation, control assessment, authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development life cycle.

Risk assessments can also address information related to the system, including system design, the intended use of the system, testing results, and supply chain-related information or artifacts. Risk assessments can play an important role in control selection processes, particularly during the application of tailoring guidance and in the earliest phases of capability determination.

Related Controls CA-3, CA-6, CM-4, CM-13, CP-6, CP-7, IA-8, MA-5, PE-3, PE-8, PE-18, PL-2, PL-10, PL-11, PM-8, PM-9, PM-28, PT-2, PT-7, RA-2, RA-5, RA-7, SA-8, SA-9, SC-38, SI-12.

JNCSF Alignment JNCSF-538 Foundational, JNCSF-539 Foundational, JNCSF-540 Foundational, JNCSF-541 Foundational, JNCSF-543 Foundational

Implementation Level I

RA-3(1) Risk Assessment | Supply Chain Risk Assessment

Control Context Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and, therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Related Controls	RA-2, RA-9, PM-17, PM-30, SR-2.
JNCSF Alignment	Additional to Jordan's National Cybersecurity Framework

Implementation Level | I

RA-5 Vulnerability Monitoring and Scanning

Control Context

Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability monitoring (including scans). Organizations determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g. switches, routers, guards, sensors), networked printers, scanners, and copiers—are not overlooked. The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability monitoring and analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools, including web-based application scanners, static analysis tools, and binary analyzers.

Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. Vulnerability monitoring may also include continuous vulnerability monitoring tools that use instrumentation to continuously analyze components. Instrumentation-based tools may improve accuracy and may be run throughout an organization without scanning. Vulnerability monitoring tools that facilitate interoperability include tools that are Security Content Automated Protocol (SCAP)-validated. Thus, organizations consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Vulnerability monitoring includes a channel and process for receiving reports of security vulnerabilities from the public at-large. Vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports, including notification authorizing good-faith research and disclosure of security vulnerabilities. Organizations generally expect that such research is happening with or without their authorization and can use public vulnerability disclosure channels to increase the likelihood that discovered vulnerabilities are reported directly to the organization for remediation.

Organizations may also employ the use of financial incentives (also known as bug bounties) to further encourage external security researchers to report discovered vulnerabilities. Bug bounty programs can be tailored to the organization’s needs. Bounties can be operated indefinitely or over a defined period of time and can be offered to the general public or to a curated group. Organizations may run public and private bounties simultaneously and could choose to offer partially credentialed access to certain participants in order to evaluate security vulnerabilities from privileged vantage points.

Related Controls CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11.

JNCSF Alignment JNCSF-307 Operation, JNCSF-308 Operation, JNCSF-309 Operation, JNCSF-310 Operation, JNCSF-311 Operation, JNCSF-312 Operation

Implementation Level 1

RA-5(2) Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned

Control Context Due to the complexity of modern software, systems, and other factors, new vulnerabilities are discovered on a regular basis. It is important that newly discovered vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner.

Related Controls SI-5.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

RA-5(4) Vulnerability Monitoring and Scanning | Discoverable Information

Control Context Discoverable information includes information that adversaries could obtain without compromising or breaching the system, such as by collecting information that the system is exposing or by conducting extensive web searches. Corrective actions include notifying appropriate organizational personnel, removing designated information, or changing the system to make the designated information less relevant or attractive to adversaries. This enhancement excludes intentionally discoverable information that may be part of a decoy capability (e.g. honeypots, honeynets, or deception nets) deployed by the organization.

Related Controls AU-13, SC-26.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access

Control Context In certain situations, the nature of the vulnerability scanning may be more intrusive, or the system component that is the subject of the scanning may contain classified or controlled unclassified information, such as personally identifiable information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

RA-5(11) Vulnerability Monitoring and Scanning | Public Disclosure Program

Control Context The reporting channel is publicly discoverable and contains clear language authorizing good-faith research and the disclosure of vulnerabilities to the organization. The organization does not condition its authorization on an expectation of indefinite non-disclosure to the public by the reporting entity but may request a specific time period to properly remediate the vulnerability.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

RA-7 Risk Response

Control Context Organizations have many options for responding to risk including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk. The risk tolerance of the organization influences risk response decisions and actions. Risk response addresses the need to determine an appropriate response to risk before generating a plan of action and milestones entry. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so that a plan of action and milestones entry is not needed. However, if the risk response is to mitigate the risk, and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

Related Controls CA-5, IR-9, PM-4, PM-28, RA-2, RA-3, SR-2.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

RA-9 Criticality Analysis

Control Context

Not all system components, functions, or services necessarily require significant protections. For example, criticality analysis is a key tenet of supply chain risk management and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, executive orders, regulations, directives, policies, standards, system functionality requirements, system and component interfaces, and system and component dependencies. Systems engineers conduct a functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities that such components create. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions that are supported by the system that contains the components and functions.

Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early in the system development life cycle, organizations may be able to modify the system design to reduce the critical nature of these components and functions, such as by adding redundancy or alternate paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is an important consideration. Such analysis is conducted as part of security categorization in RA-2.

Related Controls

CP-2, PL-2, PL-8, PL-11, PM-1, PM-11, RA-2, SA-8, SA-15, SA-20, SR-5.

JNCSF Alignment

Additional to Jordan's National Cybersecurity Framework

15 CONTROL FAMILY: SYSTEM AND SERVICES ACQUISITION

Implementation Level | 1

SA-1 Policy and Procedures

Control Context System and services acquisition policy and procedures address the controls in the SA 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 system and services acquisition 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 that reflect 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and services acquisition policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls PM-9, PS-8, SA-8, SI-12.

JNCSF Alignment JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level | 1

SA-2 Allocation of Resources

Control Context Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain-related risks throughout the system development life cycle.

Related Controls PL-7, PM-3, PM-11, SA-9, SR-3, SR-5.

JNCSF Alignment JNCSF-20 Security in Architecture and Portfolio, JNCSF-316 Operation, JNCSF-317 Operation

Implementation Level | I

SA-3 System Development Life Cycle

Control Context

A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational systems. The integration of security and privacy considerations early in the system development life cycle is a foundational principle of systems security engineering and privacy engineering. To apply the required controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical mission and business functions. The security engineering principles in SA-8 help individuals properly design, code, and test systems and system components. Organizations include qualified personnel (e.g. senior agency information security officers, senior agency officials for privacy, security and privacy architects, and security and privacy engineers) in system development life cycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. Role-based security and privacy training programs can ensure that individuals with key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development life cycle activities.

The effective integration of security and privacy requirements into enterprise architecture also helps to ensure that important security and privacy considerations are addressed throughout the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with the risk management strategy of the organization. Because the system development life cycle involves multiple organizations, (e.g. external suppliers, developers, integrators, service providers), acquisition and supply chain risk management functions and controls play significant roles in the effective management of the system during the life cycle.

Related Controls AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-15, SA-17, SA-22, SR-3, SR-4, SR-5, SR-9.

JNCSF Alignment JNCSF-53 Development, JNCSF-54 Development, JNCSF-55 Development, JNCSF-56 Development

Implementation Level | I

SA-3(1) System Development Life Cycle | Manage Preproduction Environment

Control Context

The preproduction environment includes development, test, and integration environments. The program protection planning processes established by the Department of Defense are examples of managing the preproduction environment for defense contractors. Criticality analysis and the application of controls on developers also contribute to a more secure system development environment.

Related Controls CM-2, CM-4, RA-3, RA-9, SA-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SA-3(2) System Development Life Cycle | Use of Live or Operational Data

Control Context

Live data is also referred to as operational data. The use of live or operational data in preproduction (i.e. development, test, and integration) environments can result in significant risks to organizations. In addition, the use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Therefore, it is important for the organization to manage any additional risks that may result from the use of live or operational data. Organizations can minimize such risks by using test or dummy data during the design, development, and testing of systems, system components, and system services. Risk assessment techniques may be used to determine if the risk of using live or operational data is acceptable.

Related Controls PM-25, RA-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

SA-3(3) System Development Life Cycle | Technology Refresh

Control Context

Technology refresh planning may encompass hardware, software, firmware, processes, personnel skill sets, suppliers, service providers, and facilities. The use of obsolete or nearing obsolete technology may increase the security and privacy risks associated with unsupported components, counterfeit or repurposed components, components unable to implement security or privacy requirements, slow or inoperable components, components from untrusted sources, inadvertent personnel error, or increased complexity. Technology refreshes typically occur during the operations and maintenance stage of the system development life cycle.

Related Controls MA-6.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

SA-4 Acquisition Process

Control Context

Security and privacy functional requirements are typically derived from the high-level security and privacy requirements described in SA-2. The derived requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Assurance requirements include development processes, procedures, and methodologies as well as the evidence from development and assessment activities that provide grounds for confidence that the required functionality is implemented and possesses the required strength of mechanism. SP 800-160-1 describes the process of requirements engineering as part of the system development life cycle.

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and for reflecting the security and privacy requirements of stakeholders. Controls are selected and implemented in order to satisfy system requirements and include developer and organizational responsibilities. Controls can include technical, administrative, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for controls within the system development life cycle.

Security and privacy documentation requirements address all stages of the system development life cycle. Documentation provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement.

Related Controls CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SA-16, SA-17, SA-21, SR-3, SR-5.

JNCSF Alignment JNCSF-333 Foundational, JNCSF-544 Foundational, JNCSF-545 Foundational, JNCSF-546 Foundational, JNCSF-547 Foundational, JNCSF-548 Foundational

Implementation Level 2

SA-4(1) Acquisition Process | Functional Properties of Controls

Control Context Functional properties of security and privacy controls describe the functionality (i.e. security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SA-4(2) Acquisition Process | Design and Implementation Information for Controls

Control Context Organizations may require different levels of detail in the documentation for the design and implementation of controls in organizational systems, system components, or system services based on mission and business requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules.

The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SA-4(5) Acquisition Process | System, Component, and Service Configurations

Control Context Examples of security configurations include the U.S. Government Configuration Baseline (USGCB), Security Technical Implementation Guides (STIGs), and any limitations on functions, ports, protocols, and services. Security characteristics can include requiring that default passwords have been changed.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SA-4(9) Acquisition Process | Functions, Ports, Protocols, and Services in Use

Control Context The identification of functions, ports, protocols, and services early in the system development life cycle (e.g. during the initial requirements definition and design stages) allows organizations to influence the design of the system, system component, or system service. This early involvement in the system development life cycle helps organizations avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or requiring system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-9 describes the requirements for external system services. Organizations identify which functions, ports, protocols, and services are provided from external sources.

Related Controls CM-7, SA-9.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level	I

SA-4(12) Acquisition Process | Data Ownership

Control Context Contractors who operate a system that contains data owned by an organization initiating the contract have policies and procedures in place to remove the data from their systems and/or return the data in a time frame defined by the contract.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level	I

SA-5 System Documentation

Control Context System documentation helps personnel understand the implementation and operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used to support the management of supply chain risk, incident response, and other functions. Personnel or roles that require documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system. Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation.

Related Controls CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3.

JNCSF Alignment JNCSF-135 Delivery, JNCSF-328 Operation, JNCSF-330 Operation

Implementation Level	I

SA-8 Security and Privacy Engineering Principles

Control Context Systems security and privacy engineering principles are closely related to and implemented throughout the system development life cycle (see SA-3). Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For existing systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems.

The application of systems security and privacy engineering principles helps organizations develop trustworthy, secure, and resilient systems and reduces the susceptibility to disruptions, hazards, threats, and the creation of privacy problems for individuals. Examples of system security engineering principles include: developing layered protections; establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring controls to meet organizational needs; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk.

Organizations that apply systems security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk management decisions. System security engineering principles can also be used to protect against certain supply chain risks, including incorporating tamper-resistant hardware into a design.

Related Controls PL-8, PM-7, RA-2, RA-3, RA-9, SA-3, SA-4, SA-15, SA-17, SA-20, SC-2, SC-3, SC-32, SC-39, SR-2, SR-3, SR-4, SR-5.

JNCSF Alignment JNCSF-61 Development

Implementation Level | 1 |

SA-9 External System Services

Control Context External system services are provided by an external provider, and the organization has no direct control over the implementation of the required controls or the assessment of control effectiveness. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a certain level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust vary based on relationships between organizations and the external providers. Organizations document the basis for the trust relationships so that the relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

Related Controls AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR-5.

JNCSF Alignment JNCSF-323 Operation

Implementation Level 2

SA-9(2) External System Services | Identification of Functions, Ports, Protocols, and Services

Control Context Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

Related Controls CM-6, CM-7.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SA-10 Developer Configuration Management

Control Context Organizations consider the quality and completeness of configuration management activities conducted by developers as direct evidence of applying effective security controls. Controls include protecting the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware from unauthorized modification or destruction. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

The configuration items that are placed under configuration management include the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation. Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance stage of the system development life cycle.

Related Controls CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SI-2, SR-3, SR-4, SR-5, SR-6.

JNCSF Alignment JNCSF-63 Development, JNCSF-64 Development, JNCSF-324 Operation, JNCSF-325 Operation

Implementation Level 2

SA-11 Developer Testing and Evaluation

Control Context Developmental testing and evaluation confirms that the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. The interconnections or changes—including upgrading or replacing applications, operating systems, and firmware—may adversely affect previously implemented controls. Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as manual code review, security architecture review, and penetration testing, as well as and static analysis, dynamic analysis, binary analysis, or a hybrid of the three analysis approaches.

Developers can use the analysis approaches, along with security instrumentation and fuzzing, in a variety of tools and in source code reviews. The security and privacy assessment plans include the specific activities that developers plan to carry out, including the types of analyses, testing, evaluation, and reviews of software and firmware components; the degree of rigor to be applied; the frequency of the ongoing testing and evaluation; and the types of artifacts produced during those processes. The depth of testing and evaluation refers to the rigor and level of detail associated with the assessment process. The coverage of testing and evaluation refers to the scope (i.e. number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security and privacy assessment plans, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the system. Contracts may specify protection requirements for documentation.

Related Controls CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SA-17, SI-2, SR-5, SR-6, SR-7.

JNCSF Alignment JNCSF-66 Development, JNCSF-468 Foundational, JNCSF-469 Foundational, JNCSF-470 Foundational, JNCSF-471 Foundational

Implementation Level 2

SA-15 Development Process, Standards, and Tools

Control Context Development tools include programming languages and computer-aided design systems. Reviews of development processes include the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

Related Controls MA-6, SA-3, SA-4, SA-8, SA-10, SA-11, SR-3, SR-4, SR-5, SR-6, SR-9.

JNCSF Alignment JNCSF-72 Development, JNCSF-73 Development, JNCSF-74 Development, JNCSF-338 Operation

Implementation Level 2

SA-15(3) Development Process, Standards, and Tools | Criticality Analysis

Control Context Criticality analysis performed by the developer provides input to the criticality analysis performed by organizations. Developer input is essential to organizational criticality analysis because organizations may not have access to detailed design documentation for system components that are developed as commercial off-the-shelf products. Such design documentation includes functional specifications, high-level designs, low-level designs, source code, and hardware schematics. Criticality analysis is important for organizational systems that are designated as high value assets. High value assets can be moderate- or high-impact systems due to heightened adversarial interest or potential adverse effects on the federal enterprise. Developer input is especially important when organizations conduct supply chain criticality analyses.

Related Controls RA-9.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SA-16 Developer-provided Training

Control Context Developer-provided training applies to external and internal (in-house) developers. Training personnel is essential to ensuring the effectiveness of the controls implemented within organizational systems. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Organizations can also request training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security and privacy functions, controls, and mechanisms.

Related Controls AT-2, AT-3, PE-3, SA-4, SA-5.

JNCSF Alignment JNCSF-75 Development

Implementation Level 3

SA-17 Developer Security and Privacy Architecture and Design

Control Context Developer security and privacy architecture and design are directed at external developers, although they could also be applied to internal (in-house) development. In contrast, PL-8 is directed at internal developers to ensure that organizations develop a security and privacy architecture that is integrated with the enterprise architecture. The distinction between SA-17 and PL-8 is especially important when organizations outsource the development of systems, system components, or system services and when there is a requirement to demonstrate consistency with the enterprise architecture and security and privacy architecture of the organization. ISO 15408-2, ISO 15408-3, and SP 800-160-1 provide information on security architecture and design, including formal policy models, security-relevant components, formal and informal correspondence, conceptually simple design, and structuring for least privilege and testing.

Related Controls PL-2, PL-8, PM-7, SA-3, SA-4, SA-8, SC-7.

JNCSF Alignment JNCSF-22 Security in Architecture and Portfolio, JNCSF-76 Development, JNCSF-77 Development, JNCSF-78 Development

Implementation Level 3

SA-21 Developer Screening

Control Context Developer screening is directed at external developers. Internal developer screening is addressed by PS-3. Because the system, system component, or system service may be used in critical activities essential to the national or economic security interests of the United States, organizations have a strong interest in ensuring that developers are trustworthy. The degree of trust required of developers may need to be consistent with that of the individuals who access the systems, system components, or system services once deployed. Authorization and personnel screening criteria include clearances, background checks, citizenship, and nationality. Developer trustworthiness may also include a review and analysis of company ownership and relationships that the company has with entities that may potentially affect the quality and reliability of the systems, components, or services being developed. Satisfying the required access authorizations and personnel screening criteria includes providing a list of all individuals who are authorized to perform development activities on the selected system, system component, or system service so that organizations can validate that the developer has satisfied the authorization and screening requirements.

Related Controls PS-2, PS-3, PS-6, PS-7, SA-4, SR-6.

JNCSF Alignment JNCSF-81 Development, JNCSF-513 Foundational

Implementation Level 1

SA-22 Unsupported System Components

Control Context Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business functions. If necessary, organizations can establish in-house support by developing customized patches for critical software components or, alternatively, obtain the services of external providers who provide ongoing support for the designated unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. The increased risk of using unsupported system components can be mitigated, for example, by prohibiting the connection of such components to public or uncontrolled networks, or implementing other forms of isolation.

Related Controls	PL-2, SA-3.
JNCSF Alignment	JNCSF-345 Operation, JNCSF-561 Foundational

16 CONTROL FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

Implementation Level 1

SC-1 Policy and Procedures

Control Context

System and communications protection policy and procedures address the controls in the SC 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 system and communications protection 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 that reflect 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and communications protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls

PM-9, PS-8, SA-8, SI-12.

JNCSF Alignment

JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-438 Foundational, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level 2

SC-2 Separation of System and User Functionality

Control Context

System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is physical or logical. Organizations may separate system management functions from user functions by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. Separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles.

Related Controls AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.

JNCSF Alignment JNCSF-346 Operation,

Implementation Level 3

SC-3 Security Function Isolation

Control Context Security functions are isolated from nonsecurity functions by means of an isolation boundary implemented within a system via partitions and domains. The isolation boundary controls access to and protects the integrity of the hardware, software, and firmware that perform system security functions. Systems implement code separation in many ways, such as through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that protect the code on disk and address space protections that protect executing code. Systems can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the ideal is for all code within the defined security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions as an exception. The isolation of security functions from nonsecurity functions can be achieved by applying the systems security engineering design principles in SA-8, including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14), and SA-8(18).

Related Controls AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC-32, SC-39, SI-16.

JNCSF Alignment JNCSF-347 Operation

Implementation Level 2

SC-4 Information in Shared System Resources

Control Context Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels), where shared system resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

Related Controls AC-3, AC-4, SA-8.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

SC-5 Denial-of-service Protection

Control Context Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a wide range of network protocols (e.g. IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events.

Related Controls CP-2, IR-4, SC-6, SC-7, SC-40.

JNCSF Alignment JNCSF-349 Operation

Implementation Level 1

SC-7 Boundary Protection

Control Context 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, and 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).

Related Controls 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.

JNCSF Alignment JNCSF-351 Operation, JNCSF-352 Operation

Implementation Level 2

SC-7(3) Boundary Protection | Access Points

Control Context

Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. Such system transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SC-7(4) Boundary Protection | External Telecommunications Services

Control Context

External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols. See SP 800-189 for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements.

Related Controls AC-3, SC-8, SC-20, SC-21, SC-22.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SC-7(5) Boundary Protection | Deny by Default — Allow by Exception

Control Context

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 a system that is connected to an external system.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SC-7(7) Boundary Protection | Split Tunneling for Remote Devices

Control Context

Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices and simultaneously, access uncontrolled networks. Split tunneling might be desirable by remote users to communicate with local system resources, such as printers or file servers. However, split tunneling can facilitate unauthorized external connections, making the system vulnerable to attack and to exfiltration of organizational information. Split tunneling can be prevented by disabling configuration settings that allow such capability in remote devices and by preventing those configuration settings from being configurable by users. Prevention can also be achieved by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments, or to a specific set of pre-approved addresses, without user control.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SC-7(8) Boundary Protection | Route Traffic to Authenticated Proxy Servers

Control Context

External networks are networks outside of organizational control. A proxy server is a server (i.e. system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. System resources that may be requested include files, connections, web pages, or services. Client requests established through a connection to a proxy server are assessed to manage complexity and provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers that provide access to the Internet. Proxy servers can support the logging of Transmission Control Protocol sessions and the blocking of specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Note that proxy servers may inhibit the use of virtual private networks (VPNs) and create the potential for man-in-the-middle attacks (depending on the implementation).

Related Controls AC-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SC-7(16) Boundary Protection | Prevent Discovery of System Components

Control Context Preventing the discovery of system components representing a managed interface helps protect network addresses of those components from discovery through common tools and techniques used to identify devices on networks. Network addresses are not available for discovery and require prior knowledge for access. Preventing the discovery of components and devices can be accomplished by not publishing network addresses, using network address translation, or not entering the addresses in domain name systems. Another prevention technique is to periodically change network addresses.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SC-7(18) Boundary Protection | Fail Secure

Control Context Fail secure is a condition achieved by employing mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces, systems do not enter into unsecure states where intended security properties no longer hold. Managed interfaces include routers, firewalls, and application gateways that reside on protected subnetworks (commonly referred to as demilitarized zones). Failures of boundary protection devices cannot lead to or cause information external to the devices to enter the devices nor can failures permit unauthorized information releases.

Related Controls CP-2, CP-12, SC-24.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SC-7(21) Boundary Protection | Isolation of System Components

Control Context Organizations can isolate system components that perform different mission or business functions. Such isolation limits unauthorized information flows among system components and provides the opportunity to deploy greater levels of protection for selected system components. Isolating system components with boundary protection mechanisms provides the capability for increased protection of individual system components and to more effectively control information flows between those components. Isolating system components provides enhanced protection that limits the potential harm from hostile cyber-attacks and errors. The degree of isolation varies depending upon the mechanisms chosen. Boundary protection mechanisms include routers, gateways, and firewalls that separate system components into physically separate networks or subnetworks; cross-domain devices that separate subnetworks; virtualization techniques; and the encryption of information flows among system components using distinct encryption keys.

Related Controls CA-9.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

SC-7(28) Boundary Protection | Connections to Public Networks

Control Context A direct connection is a dedicated physical or virtual connection between two or more systems. A public network is a network accessible to the public, including the Internet and organizational extranets with public access.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SC-7(29) Boundary Protection | Separate Subnets to Isolate Functions

Control Context Separating critical system components and functions from other noncritical system components and functions through separate subnetworks may be necessary to reduce susceptibility to a catastrophic or debilitating breach or compromise that results in system failure. For example, physically separating the command and control function from the in-flight entertainment function through separate subnetworks in a commercial aircraft provides an increased level of assurance in the trustworthiness of critical system functions.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SC-8 Transmission Confidentiality and Integrity

Control Context Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques.

Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls.

Related Controls AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SA-8, SC-7, SC-16, SC-20, SC-23, SC-28.

JNCSF Alignment JNCSF-354 Operation

Implementation Level 2

SC-8(1) Transmission Confidentiality and Integrity | Cryptographic Protection

Control Context Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPSec. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

Related Controls SC-12, SC-13.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

SC-12 Cryptographic Key Establishment and Management

Control Context 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.

Related Controls 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.

JNCSF Alignment JNCSF-360 Operation, JNCSF-362 Operation, JNCSF-363 Operation, JNCSF-364 Operation, JNCSF-365 Operation

Implementation Level 3

SC-12(1) Cryptographic Key Establishment and Management | Availability

Control Context Escrowing of encryption keys is a common practice for ensuring availability in the event of key loss. A forgotten passphrase is an example of losing a cryptographic key.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

SC-13 Cryptographic Protection

Control Context 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.

Related Controls 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.

JNCSF Alignment JNCSF-565 Foundational

Implementation Level 1

SC-15 Collaborative Computing Devices and Applications

Control Context Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.

Related Controls AC-21, SC-42.

JNCSF Alignment JNCSF-368 Operation

Implementation Level 2

SC-17 Public Key Infrastructure Certificates

Control Context Public key infrastructure (PKI) certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e. a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates.

Related Controls AU-10, IA-5, SC-12.

JNCSF Alignment JNCSF-361 Operation

Implementation Level 2

SC-18 Mobile Code

Control Context Mobile code includes any program, application, or content that can be transmitted across a network (e.g. embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

Related Controls AU-2, AU-12, CM-2, CM-6, SI-3.

JNCSF Alignment JNCSF-370 Operation, JNCSF-371 Operation, JNCSF-372 Operation

Implementation Level 1

SC-20 Secure Name/address Resolution Service (authoritative Source)

Control Context Providing authoritative source information enables external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include domain name system (DNS) servers. Additional artifacts include DNS Security Extensions (DNSSEC) digital signatures and cryptographic keys. Authoritative data includes DNS resource records. The means for indicating the security status of child zones include the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data.

Related Controls AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

JNCSF Alignment JNCSF-374 Operation, JNCSF-375 Operation

Implementation Level I

SC-21 Secure Name/address Resolution Service (recursive or Caching Resolver)

Control Context Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

Related Controls SC-20, SC-22.

JNCSF Alignment JNCSF-376 Operation

Implementation Level I

SC-22 Architecture and Provisioning for Name/address Resolution Service

Control Context Systems that provide name and address resolution services include domain name system (DNS) servers. To eliminate single points of failure in systems and enhance redundancy, organizations employ at least two authoritative domain name system servers—one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e. not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e. from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e. on external networks, including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles (e.g. by address ranges and explicit lists).

Related Controls SC-2, SC-20, SC-21, SC-24.

JNCSF Alignment JNCSF-377 Operation

Implementation Level 2

SC-23 Session Authenticity

Control Context Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into sessions.

Related Controls AU-10, SC-8, SC-10, SC-11.

JNCSF Alignment JNCSF-378 Operation

Implementation Level 3

SC-24 Fail in Known State

Control Context Failure in a known state addresses security concerns in accordance with the mission and business needs of organizations. Failure in a known state prevents the loss of confidentiality, integrity, or availability of information in the event of failures of organizational systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving system state information facilitates system restart and return to the operational mode with less disruption of mission and business processes.

Related Controls CP-2, CP-4, CP-10, CP-12, SA-8, SC-7, SC-22, SI-13.

JNCSF Alignment JNCSF-379 Operation

Implementation Level 2

SC-28 Protection of Information at Rest

Control Context 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.

Related Controls 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.

JNCSF Alignment JNCSF-382 Operation

Implementation Level 2

SC-28(1) Protection of Information at Rest | Cryptographic Protection

Control Context The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields.

Related Controls AC-19, SC-12, SC-13.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SC-29 Heterogeneity

Control Context Increasing the diversity of information technologies within organizational systems reduces the impact of potential exploitations or compromises of specific technologies. Such diversity protects against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one system component will be effective against other system components, thus further increasing the adversary work factor to successfully complete planned attacks. An increase in diversity may add complexity and management overhead that could ultimately lead to mistakes and unauthorized configurations.

Related Controls AU-9, PL-8, SC-27, SC-30, SR-3.

JNCSF Alignment JNCSF-383 - Operation

Implementation Level 3

SC-30 Concealment and Misdirection

Control Context

Concealment and misdirection techniques can significantly reduce the targeting capabilities of adversaries (i.e. window of opportunity and available attack surface) to initiate and complete attacks. For example, virtualization techniques provide organizations with the ability to disguise systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. The increased use of concealment and misdirection techniques and methods—including randomness, uncertainty, and virtualization—may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment and misdirection techniques may provide additional time to perform core mission and business functions. The implementation of concealment and misdirection techniques may add to the complexity and management overhead required for the system.

Related Controls AC-6, SC-25, SC-26, SC-29, SC-44, SI-14

JNCSF Alignment JNCSF-384 - Operation

Implementation Level 3

SC-31 Covert Channel Analysis

Control Context

Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, such as in the case of systems that contain export-controlled information and have connections to external networks (i.e. networks that are not controlled by organizations). Covert channel analysis is also useful for multilevel secure systems, multiple security level systems, and cross-domain systems.

Related Controls AC-3, AC-4, SA-8, SI-11.

JNCSF Alignment JNCSF-385 - Operation

Implementation Level 1

SC-39 Process Isolation

Control Context

Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. Process isolation helps limit the access of potentially untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies.

Related Controls AC-3, AC-4, AC-6, AC-25, SA-8, SC-2, SC-3, SI-16.

JNCSF Alignment JNCSF-352 Operation, JNCSF-353 Operation

Implementation Level 2

SC-41 Port and I/O Device Access

Control Context Connection ports include Universal Serial Bus (USB), Thunderbolt, and Firewire (IEEE 1394). Input/output (I/O) devices include compact disc and digital versatile disc drives. Disabling or removing such connection ports and I/O devices helps prevent the exfiltration of information from systems and the introduction of malicious code from those ports or devices. Physically disabling or removing ports and/or devices is the stronger action.

Related Controls AC-20, MP-7.

JNCSF Alignment JNCSF-401 Operation

Implementation Level 3

SC-44 Detonation Chambers

Control Context Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator requests in the safety of an isolated environment or a virtualized sandbox. Protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code. While related to the concept of deception nets, the employment of detonation chambers is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, detonation chambers are intended to quickly identify malicious code and either reduce the likelihood that the code is propagated to user environments of operation or prevent such propagation completely.

Related Controls SC-7, SC-18, SC-25, SC-26, SC-30, SC-35, SC-39, SI-3, SI-7

JNCSF Alignment JNCSF-406 - Operation

Implementation Level | I

SC-45 System Time Synchronization

Control Context

Time synchronization of system clocks is essential for the correct execution of many system services, including identification and authentication processes that involve certificates and time-of-day restrictions as part of access control. Denial of service or failure to deny expired credentials may result without properly synchronized clocks within and between systems and system components. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, such as clocks synchronizing within hundreds of milliseconds or tens of milliseconds. Organizations may define different time granularities for system components. Time service can be critical to other security capabilities—such as access control and identification and authentication—depending on the nature of the mechanisms used to support the capabilities.

Related Controls AC-3, AU-8, IA-2, IA-8.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | I

SC-45(1) System Time Synchronization | Synchronization with Authoritative Time Source

Control Context

Synchronization of internal system clocks with an authoritative source provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

17 CONTROL FAMILY: SYSTEM AND INFORMATION INTEGRITY

Implementation Level	I

SI-1 Policy and Procedures

Control Context

System and information integrity policy and procedures address the controls in the SI 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 system and information integrity 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 that reflect 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls

PM-9, PS-8, SA-8, SI-12.

JNCSF Alignment

JNCSF-1 Security in Architecture and Portfolio, JNCSF-2 Security in Architecture and Portfolio, JNCSF-439 Foundational, JNCSF-571 Foundational

Implementation Level	I

SI-2 Flaw Remediation

Control Context

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.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e. severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment. Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software or firmware updates is not necessary or practical, such as when implementing simple malicious code signature updates. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Related Controls 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.

JNCSF Alignment JNCSF-86 Development, JNCSF-407 Operation, JNCSF-408 Operation, JNCSF-567 Foundational

Implementation Level 2

SI-2(2) Flaw Remediation | Automated Flaw Remediation Status

Control Context Automated mechanisms can track and determine the status of known flaws for system components.

Related Controls CA-7, SI-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

SI-3 Malicious Code Protection

Control Context System entry and exit points include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the world-wide web, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code.

Malicious code protection mechanisms include both signature- and nonsignature-based technologies. Nonsignature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e. code that changes signatures when it replicates). Nonsignature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software as well as custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.

In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended. Organizations may determine that, in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, the detection of malicious downloads, or the detection of maliciousness when attempting to open or execute files.

Related Controls 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.

JNCSF Alignment JNCSF-87 Development, JNCSF-88 Development, JNCSF-89 Development, JNCSF-90 Development, JNCSF-91 Development

Implementation Level 1

SI-4 System Monitoring

Control Context 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. Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls 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.

JNCSF Alignment JNCSF-409 Operation, JNCSF-410 Operation, JNCSF-411 Operation, JNCSF-412 Operation, JNCSF-413 Operation, JNCSF-414 Operation, JNCSF-415 Operation, JNCSF-

568 Foundational, JNCSF-569 Foundational

Implementation Level 2

SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-time Analysis

Control Context Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or Security Information and Event Management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls PM-23, PM-25.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic

Control Context Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SI-4(5) System Monitoring | System-generated Alerts

Control Context Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations in SI-4(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

Related Controls AU-4, AU-5, PE-6.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SI-4(10) System Monitoring | Visibility of Encrypted Communications

Control Context Organizations balance the need to encrypt communications traffic to protect data confidentiality with the need to maintain visibility into such traffic from a monitoring perspective. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SI-4(12) System Monitoring | Automated Organization-generated Alerts

Control Context Organizational personnel on the system alert notification list include system administrators, mission or business owners, system owners, senior agency information security officer, senior agency official for privacy, system security officers, or privacy officers. Automated organization-generated alerts are the security alerts generated by organizations and transmitted using automated means. The sources for organization-generated alerts are focused on other entities such as suspicious activity reports and reports on potential insider threats. In contrast to alerts generated by the organization, alerts generated by the system in SI-4(5) focus on information sources that are internal to the systems, such as audit records.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SI-4(14) System Monitoring | Wireless Intrusion Detection

Control Context Wireless signals may radiate beyond organizational facilities. Organizations proactively search for unauthorized wireless connections, including the conduct of thorough scans for unauthorized wireless access points. Wireless scans are not limited to those areas within facilities containing systems but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational systems.

Related Controls AC-18, IA-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SI-4(20) System Monitoring | Privileged Users

Control Context Privileged users have access to more sensitive information, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to systems and organizations than non-privileged users. Therefore, implementing additional monitoring on privileged users helps to ensure that organizations can identify malicious activity at the earliest possible time and take appropriate actions.

Related Controls AC-18.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SI-4(22) System Monitoring | Unauthorized Network Services

Control Context Unauthorized or unapproved network services include services in service-oriented architectures that lack organizational verification or validation and may therefore be unreliable or serve as malicious rogues for valid services.

Related Controls CM-7.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

#

Implementation Level | 1

SI-5 Security Alerts, Advisories, and Directives

Control Context NCSC-Jo may generates security alerts and advisories to maintain situational awareness throughout their portal. Compliance with local law is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations.

Related Controls PM-15, RA-5, SI-2.

JNCSF Alignment JNCSF-416 Operation, JNCSF-417 Operation, JNCSF-418 Operation

Implementation Level | 3

SI-5(1) Security Alerts, Advisories, and Directives | Automated Alerts and Advisories

Control Context The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational mission and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three levels related to the management of risk, including the governance level, mission and business process level, and the information system level.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | 3

SI-6 Security and Privacy Function Verification

Control Context Transitional states for systems include system startup, restart, shutdown, and abort. System notifications include hardware indicator lights, electronic alerts to system administrators, and messages to local computer consoles. In contrast to security function verification, privacy function verification ensures that privacy functions operate as expected and are approved by the senior agency official for privacy or that privacy attributes are applied or used as expected.

Related Controls CA-7, CM-4, CM-6, SI-7.

JNCSF Alignment JNCSF-92 Development, JNCSF-136 Delivery

Implementation Level 2

SI-7 Software, Firmware, and Information Integrity

Control Context Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

Related Controls AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11.

JNCSF Alignment JNCSF-419 Operation

Implementation Level 2

SI-7(1) Software, Firmware, and Information Integrity | Integrity Checks

Control Context Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SI-7(2) Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations

Control Context The employment of automated tools to report system and information integrity violations and to notify organizational personnel in a timely matter is essential to effective risk response. Personnel with an interest in system and information integrity violations include mission and business owners, system owners, senior agency information security official, senior agency official for privacy, system administrators, software developers, systems integrators, information security officers, and privacy officers.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations

Control Context Organizations may define different integrity-checking responses by type of information, specific information, or a combination of both. Types of information include firmware, software, and user data. Specific information includes boot firmware for certain types of machines. The automatic implementation of controls within organizational systems includes reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response

Control Context Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

Related Controls AU-2, AU-6, IR-4, IR-5, SI-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SI-7(15) Software, Firmware, and Information Integrity | Code Authentication

Control Context Cryptographic authentication includes verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code. Organizations that employ cryptographic mechanisms also consider cryptographic key management solutions.

Related Controls CM-5, SC-12, SC-13.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SI-8 Spam Protection

Control Context System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions.

Related Controls PL-9, SC-5, SC-7, SC-38, SI-3, SI-4.

JNCSF Alignment JNCSF-420 Operation, JNCSF-421 Operation

Implementation Level 2

SI-8(2) Spam Protection | Automatic Updates

Control Context Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capabilities.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SI-10 Information Input Validation

Control Context Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of 387, abc, or %K% are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e. commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

Related Controls None.

JNCSF Alignment JNCSF-422 Operation

Implementation Level 2

SI-11 Error Handling

Control Context Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

Related Controls AU-2, AU-3, SC-31, SI-2, SI-15.

JNCSF Alignment JNCSF-423 Operation,
JNCSF-424 Operation

Implementation Level 1

SI-12 Information Management and Retention

Control Context Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative information. NCSC-JO or regulators could provide policy and guidance on records retention and schedules. If organizations have a records management office, consider coordinating with records management personnel.

Related Controls AC-16, AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM-5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PL-2, PL-4, PM-4, PM-8, PM-9, PS-2, PS-6, PT-2, PT-3, RA-2, RA-3, SA-5, SA-8, SR-2.

JNCSF Alignment JNCSF-425 Operation

Implementation Level 3

SI-15 Information Output Filtering

Control Context Certain types of attacks, including SQL injections, produce output results that are unexpected or inconsistent with the output results that would be expected from software programs or applications. Information output filtering focuses on detecting extraneous content, preventing such extraneous content from being displayed, and then alerting monitoring tools that anomalous behavior has been discovered.

Related Controls SI-3, SI-4, SI-11.

JNCSF Alignment JNCSF-93 - Development

Implementation Level 2

SI-16 Memory Protection

Control Context Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

Related Controls AC-25, SC-3, SI-7.

JNCSF Alignment JNCSF-94 Development

Implementation Level 2

SI-17 Fail-safe Procedures

Control Context Failure conditions include the loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include alerting operator personnel and providing specific instructions on subsequent steps to take. Subsequent steps may include doing nothing, reestablishing system settings, shutting down processes, restarting the system, or contacting designated organizational personnel.

Related Controls CP-12, CP-13, SC-24, SI-13.

JNCSF Alignment JNCSF-24 Security in Architecture and Portfolio

18 CONTROL FAMILY: SUPPLY CHAIN RISK MANAGEMENT

Implementation Level | 1

SR-1 Policy and Procedures

Control Context

Supply chain risk management policy and procedures address the controls in the SR family as well as supply chain-related controls in other families 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 supply chain risk management 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 that reflect 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. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to supply chain risk management policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls PM-9, PM-30, PS-8, SI-12.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level | 1

SR-2 Supply Chain Risk Management Plan

Control Context

The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders. Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints and implications. It can either be stand-alone, or incorporated into system security and privacy plans. The SCRM plan addresses managing, implementation, and monitoring of SCRM controls and the development/sustainment of systems across the

SDLC to support mission and business functions.

Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose, and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment. Supply chain risk management plans include an expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, a description of and justification for supply chain risk mitigation measures taken, and associated roles and responsibilities. Finally, supply chain risk management plans address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes (see SA-8).

Related Controls CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SR-2(1) Supply Chain Risk Management Plan | Establish SCRM Team

Control Context To implement supply chain risk management plans, organizations establish a coordinated, team-based approach to identify and assess supply chain risks and manage these risks by using programmatic and technical mitigation techniques. The team approach enables organizations to conduct an analysis of their supply chain, communicate with internal and external partners or stakeholders, and gain broad consensus regarding the appropriate resources for SCRM. The SCRM team consists of organizational personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executive, information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions. Members of the SCRM team are involved in various aspects of the SDLC and, collectively, have an awareness of and provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems. The SCRM team can be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

Related Controls None.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

SR-3 Supply Chain Controls and Processes

Control Context

Supply chain elements include organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components. Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components. Supply chain elements and processes may be provided by organizations, system integrators, or external providers. Weaknesses or deficiencies in supply chain elements or processes represent potential vulnerabilities that can be exploited by adversaries to cause harm to the organization and affect its ability to carry out its core missions or business functions. Supply chain personnel are individuals with roles and responsibilities in the supply chain.

Related Controls

CA-2, MA-2, MA-6, PE-3, PE-16, PL-8, PM-30, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SC-7, SC-29, SC-30, SC-38, SI-7, SR-6, SR-9, SR-11.

JNCSF Alignment

Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SR-3(1) Supply Chain Controls and Processes | Diverse Supply Base

Control Context

Diversifying the supply of systems, system components, and services can reduce the probability that adversaries will successfully identify and target the supply chain and can reduce the impact of a supply chain event or compromise. Identifying multiple suppliers for replacement components can reduce the probability that the replacement component will become unavailable. Employing a diverse set of developers or logistics service providers can reduce the impact of a natural disaster or other supply chain event. Organizations consider designing the system to include diverse materials and components.

Related Controls

None.

JNCSF Alignment

Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SR-4 Provenance

Control Context

: Every system and system component has a point of origin and may be changed throughout its existence. Provenance is the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. Organizations consider developing procedures (see SR-1) for allocating responsibilities for the creation, maintenance, and monitoring of provenance for systems and system components; transferring provenance documentation and responsibility between organizations; and preventing and monitoring for unauthorized changes to the provenance records. Organizations have methods to document, monitor, and maintain valid provenance baselines for systems, system components, and related data. These actions help track, assess, and document any changes to the provenance, including changes in supply chain elements or configuration, and help ensure non-repudiation of provenance information and the provenance change records. Provenance considerations are addressed throughout the system development life cycle and incorporated into contracts and other arrangements, as appropriate.

Related Controls CM-8, MA-2, MA-6, RA-9, SA-3, SA-8, SI-4.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level I

SR-5 Acquisition Strategies, Tools, and Methods

Control Context The use of the acquisition process provides an important vehicle to protect the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development life cycle. Organizations also consider providing incentives for suppliers who implement controls, promote transparency into their processes and security and privacy practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.

Related Controls AT-3, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SR-6, SR-9, SR-10, SR-11.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SR-5(1) Acquisition Strategies, Tools, and Methods | Adequate Supply

Control Context Adversaries can attempt to impede organizational operations by disrupting the supply of critical system components or corrupting supplier operations. Organizations may track systems and component mean time to failure to mitigate the loss of temporary or permanent system function. Controls to ensure that adequate supplies of critical system components include the use of multiple suppliers throughout the supply chain for the identified critical components, stockpiling spare components to ensure operation during mission-critical times, and the identification of functionally identical or similar components that may be used, if necessary.

Related Controls RA-9.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SR-6 Supplier Assessments and Reviews

Control Context An assessment and review of supplier risk includes security and supply chain risk management processes, foreign ownership, control or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors. The reviews may be conducted by the organization or by an independent third party. The reviews consider documented processes, documented controls, all-source intelligence, and publicly available information related to the supplier or contractor. Organizations can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits. In some cases, it may be appropriate or required to share assessment and review results with other organizations in accordance with any applicable rules, policies, or inter-organizational agreements or contracts.

Related Controls SR-3, SR-5.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

SR-8 Notification Agreements

Control Context The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

Related Controls IR-4, IR-6, IR-8.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SR-9 Tamper Resistance and Detection

Control Context Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.

Related Controls PE-3, PM-30, SA-15, SI-4, SI-7, SR-3, SR-4, SR-5, SR-10, SR-11.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 3

SR-9(1) Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle

Control Context The system development life cycle includes research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal. Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations use obfuscation and self-checking to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. The customization of systems and system components can make substitutions easier to detect and therefore limit damage.

Related Controls SA-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

SR-10 Inspection of Systems or Components

Control Context The inspection of systems or systems components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from organization-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

Related Controls AT-3, PM-30, SI-4, SI-7, SR-3, SR-4, SR-5, SR-9, SR-11.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

SR-11 Component Authenticity

Control Context Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include NCSC-JO.

Related Controls PE-3, SA-4, SI-7, SR-9, SR-10.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SR-11(1) Component Authenticity | Anti-counterfeit Training

Control Context None.

Related Controls AT-3.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 2

SR-11(2) Component Authenticity | Configuration Control for Component Service and Repair

Control Context None.

Related Controls CM-3, MA-2, MA-4, SA-10.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

Implementation Level 1

SR-12 Component Disposal

Control Context

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 of the life cycle). 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, 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, which contain sensitive or proprietary information. Additionally, proper disposal of system components helps to prevent such components from entering the gray market.

Related Controls MP-6.

JNCSF Alignment Additional to Jordan's National Cybersecurity Framework

المركـز الوطنـي للأمـن السيبرانــي

National Cyber Security Center