3.18 SYSTEM AND COMMUNICATIONS PROTECTION

Quick link to System and Communications Protection Summary Table

SC-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] system and communications protection policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

c. Review and update the current system and communications protection:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: 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.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-100].

SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

Control: Separate user functionality, including user interface services, from system management functionality.

Discussion: 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 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-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.

Control Enhancements:

(1) SEPARATION OF SYSTEM AND USER FUNCTIONALITY | INTERFACES FOR NON-PRIVILEGED USERS

Prevent the presentation of system management functionality at interfaces to non-privileged users.

Discussion: Preventing the presentation of system management functionality at interfaces to non-privileged users ensures that system administration options, including administrator privileges, are not available to the general user population. Restricting user access also prohibits the use of the grey-out option commonly used to eliminate accessibility to such information. One potential solution is to withhold system administration options until users establish sessions with administrator privileges.

Related Controls: AC-3.

(2) SEPARATION OF SYSTEM AND USER FUNCTIONALITY | DISASSOCIABILITY

Store state information from applications and software separately.

Discussion: If a system is compromised, storing applications and software separately from state information about users' interactions with an application may better protect individuals' privacy.

Related Controls: None.

References: None.

SC-3 SECURITY FUNCTION ISOLATION

Control: Isolate security functions from nonsecurity functions.

Discussion: 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.

Control Enhancements:

(1) SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION

Employ hardware separation mechanisms to implement security function isolation.

Discussion: Hardware separation mechanisms include hardware ring architectures that are implemented within microprocessors and hardware-enforced address segmentation used to support logically distinct storage objects with separate attributes (i.e., readable, writeable).

Related Controls: None.

(2) SECURITY FUNCTION ISOLATION | ACCESS AND FLOW CONTROL FUNCTIONS

Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.

Discussion: Security function isolation occurs because of implementation. The functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include auditing, intrusion detection, and malicious code protection functions.

Related Controls: None.

(3) SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY

Minimize the number of nonsecurity functions included within the isolation boundary containing security functions.

Discussion: Where it is not feasible to achieve strict isolation of nonsecurity functions from security functions, it is necessary to take actions to minimize nonsecurity-relevant functions within the security function boundary. Nonsecurity functions contained within the isolation boundary are considered security-relevant because errors or malicious code in the software can directly impact the security functions of systems. The fundamental design objective is that the specific portions of systems that provide information security are of minimal size and complexity. Minimizing the number of nonsecurity functions in the security-relevant system components allows designers and implementers to focus only on those functions which are necessary to provide the desired security capability (typically access enforcement). By minimizing the nonsecurity functions within the isolation boundaries, the amount of code that is trusted to enforce security policies is significantly reduced, thus contributing to understandability.

Related Controls: None.

(4) SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS

Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.

Discussion: The reduction of inter-module interactions helps to constrain security functions and manage complexity. The concepts of coupling and cohesion are important with respect to modularity in software design. Coupling refers to the dependencies that one module has on other modules. Cohesion refers to the relationship between functions within a module. Best practices in software engineering and systems security engineering rely on layering,

minimization, and modular decomposition to reduce and manage complexity. This produces software modules that are highly cohesive and loosely coupled.

Related Controls: None.

(5) SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES

Implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

Discussion: The implementation of layered structures with minimized interactions among security functions and non-looping layers (i.e., lower-layer functions do not depend on higher-layer functions) enables the isolation of security functions and the management of complexity.

Related Controls: None.

References: None.

SC-4 INFORMATION IN SHARED SYSTEM RESOURCES

Control: Prevent unauthorized and unintended information transfer via shared system resources.

Discussion: 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.

Control Enhancements:

(1) INFORMATION IN SHARED SYSTEM RESOURCES | SECURITY LEVELS

[Withdrawn: Incorporated into SC-4.]

(2) INFORMATION IN SHARED SYSTEM RESOURCES | MULTILEVEL OR PERIODS PROCESSING

Prevent unauthorized information transfer via shared resources in accordance with [*Assignment: organization-defined procedures*] when system processing explicitly switches between different information classification levels or security categories.

Discussion: Changes in processing levels can occur during multilevel or periods processing with information at different classification levels or security categories. It can also occur during serial reuse of hardware components at different classification levels. Organization-defined procedures can include approved sanitization processes for electronically stored information.

Related Controls: None.

References: None.

SC-5 DENIAL-OF-SERVICE PROTECTION

Control:

a. [*Selection: Protect against; Limit*] the effects of the following types of denial-of-service events: [*Assignment: organization-defined types of denial-of-service events*]; and

b. Employ the following controls to achieve the denial-of-service objective: [*Assignment: organization-defined controls by type of denial-of-service event*].

Discussion: 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.

Control Enhancements:

(1) DENIAL-OF-SERVICE PROTECTION | RESTRICT ABILITY TO ATTACK OTHER SYSTEMS

Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: [*Assignment: organization-defined denial-of-service attacks*].

Discussion: Restricting the ability of individuals to launch denial-of-service attacks requires the mechanisms commonly used for such attacks to be unavailable. Individuals of concern include hostile insiders or external adversaries who have breached or compromised the system and are using it to launch a denial-of-service attack. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., wired networks, wireless networks, spoofed Internet protocol packets). Organizations can also limit the ability of individuals to use excessive system resources. Protection against individuals having the ability to launch denial-of-service attacks may be implemented on specific systems or boundary devices that prohibit egress to potential target systems.

Related Controls: None.

(2) DENIAL-OF-SERVICE PROTECTION | CAPACITY, BANDWIDTH, AND REDUNDANCY

Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.

Discussion: Managing capacity ensures that sufficient capacity is available to counter flooding attacks. Managing capacity includes establishing selected usage priorities, quotas, partitioning, or load balancing.

Related Controls: None.

(3) DENIAL-OF-SERVICE PROTECTION | DETECTION AND MONITORING

(a) Employ the following monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: [*Assignment: organization-defined monitoring tools*]; and

(b) Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: [*Assignment: organization-defined system resources*].

Discussion: Organizations consider the utilization and capacity of system resources when managing risk associated with a denial of service due to malicious attacks. Denial-of-service attacks can originate from external or internal sources. System resources that are sensitive to denial of service include physical disk storage, memory, and CPU cycles. Techniques used to prevent denial-of-service attacks related to storage utilization and capacity include instituting disk quotas, configuring systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data.

Related Controls: CA-7, SI-4.

References: [SP 800-189].

SC-6 RESOURCE AVAILABILITY

Control: Protect the availability of resources by allocating [*Assignment: organization-defined resources*] by [*Selection (one or more): priority; quota;* [*Assignment: organization-defined controls*]].

Discussion: Priority protection prevents lower-priority processes from delaying or interfering with the system that services higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources.

Related Controls: SC-5.

Control Enhancements: None.

References: [OMB M-08-05], [DHS TIC].

SC-7 BOUNDARY PROTECTION

Control:

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

b. Implement subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

Discussion: 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.

Control Enhancements:

(1) BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS

[Withdrawn: Incorporated into SC-7.]

(2) BOUNDARY PROTECTION | PUBLIC ACCESS

[Withdrawn: Incorporated into SC-7.]

(3) BOUNDARY PROTECTION | ACCESS POINTS

Limit the number of external network connections to the system.

Discussion: Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. The Trusted Internet Connection [DHS TIC] initiative is an example of a federal guideline that requires limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such 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.

(4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES

(a) Implement a managed interface for each external telecommunication service;

(b) Establish a traffic flow policy for each managed interface;

(c) Protect the confidentiality and integrity of the information being transmitted across each interface;

(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;

(e) Review exceptions to the traffic flow policy [*Assignment: organization-defined frequency*] and remove exceptions that are no longer supported by an explicit mission or business need;

(f) Prevent unauthorized exchange of control plane traffic with external networks;

(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

(h) Filter unauthorized control plane traffic from external networks.

Discussion: 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.

(5) BOUNDARY PROTECTION | DENY BY DEFAULT — ALLOW BY EXCEPTION

Deny network communications traffic by default and allow network communications traffic by exception [*Selection (one or more): at managed interfaces; for* [*Assignment: organization-defined systems*]].

Discussion: 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.

(6) BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES

[Withdrawn: Incorporated into SC-7(18).]

(7) BOUNDARY PROTECTION | SPLIT TUNNELING FOR REMOTE DEVICES

Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [*Assignment: organization-defined safeguards*].

Discussion: 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.

(8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

Route [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers at managed interfaces.

Discussion: 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.

(9) BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC

(a) Detect and deny outgoing communications traffic posing a threat to external systems; and

(b) Audit the identity of internal users associated with denied communications.

Discussion: Detecting outgoing communications traffic from internal actions that may pose threats to external systems is known as extrusion detection. Extrusion detection is carried out within the system at managed interfaces. Extrusion detection includes the analysis of

incoming and outgoing communications traffic while searching for indications of internal threats to the security of external systems. Internal threats to external systems include traffic indicative of denial-of-service attacks, traffic with spoofed source addresses, and traffic that contains malicious code. Organizations have criteria to determine, update, and manage identified threats related to extrusion detection.

Related Controls: AU-2, AU-6, SC-5, SC-38, SC-44, SI-3, SI-4.

(10) BOUNDARY PROTECTION | PREVENT EXFILTRATION

(a) Prevent the exfiltration of information; and

(b) Conduct exfiltration tests [*Assignment: organization-defined frequency*].

Discussion: Prevention of exfiltration applies to both the intentional and unintentional exfiltration of information. Techniques used to prevent the exfiltration of information from systems may be implemented at internal endpoints, external boundaries, and across managed interfaces and include adherence to protocol formats, monitoring for beaconing activity from systems, disconnecting external network interfaces except when explicitly needed, employing traffic profile analysis to detect deviations from the volume and types of traffic expected, call backs to command and control centers, conducting penetration testing, monitoring for steganography, disassembling and reassembling packet headers, and using data loss and data leakage prevention tools. Devices that enforce strict adherence to protocol formats include deep packet inspection firewalls and Extensible Markup Language (XML) gateways. The devices verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices that operate at the network or transport layers. The prevention of exfiltration is similar to data loss prevention or data leakage prevention and is closely associated with cross-domain solutions and system guards that enforce information flow requirements.

Related Controls: AC-2, CA-8, SI-3.

(11) BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC

Only allow incoming communications from [*Assignment: organization-defined authorized sources*] to be routed to [*Assignment: organization-defined authorized destinations*].

Discussion: General source address validation techniques are applied to restrict the use of illegal and unallocated source addresses as well as source addresses that should only be used within the system. The restriction of incoming communications traffic provides determinations that source and destination address pairs represent authorized or allowed communications. Determinations can be based on several factors, including the presence of such address pairs in the lists of authorized or allowed communications, the absence of such address pairs in lists of unauthorized or disallowed pairs, or meeting more general rules for authorized or allowed source and destination pairs. Strong authentication of network addresses is not possible without the use of explicit security protocols, and thus, addresses can often be spoofed. Further, identity-based incoming traffic restriction methods can be employed, including router access control lists and firewall rules.

Related Controls: AC-3.

(12) BOUNDARY PROTECTION | HOST-BASED PROTECTION

Implement [*Assignment: organization-defined host-based boundary protection mechanisms*] at [*Assignment: organization-defined system components*].

Discussion: Host-based boundary protection mechanisms include host-based firewalls. System components that employ host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.

Related Controls: None.

(13) BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS

Isolate [*Assignment: organization-defined information security tools, mechanisms, and support components*] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

Discussion: Physically separate subnetworks with managed interfaces are useful in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques employed by organizations.

Related Controls: SC-2, SC-3.

(14) BOUNDARY PROTECTION | PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS

Protect against unauthorized physical connections at [*Assignment: organization-defined managed interfaces*].

Discussion: Systems that operate at different security categories or classification levels may share common physical and environmental controls, since the systems may share space within the same facilities. In practice, it is possible that these separate systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved by using clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls that enforce limited authorized access to these items.

Related Controls: PE-4, PE-19.

(15) BOUNDARY PROTECTION | NETWORKED PRIVILEGED ACCESSES

Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

Discussion: Privileged access provides greater accessibility to system functions, including security functions. Adversaries attempt to gain privileged access to systems through remote access to cause adverse mission or business impacts, such as by exfiltrating information or bringing down a critical system capability. Routing networked, privileged access requests through a dedicated, managed interface further restricts privileged access for increased access control and auditing.

Related Controls: AC-2, AC-3, AU-2, SI-4.

(16) BOUNDARY PROTECTION | PREVENT DISCOVERY OF SYSTEM COMPONENTS

Prevent the discovery of specific system components that represent a managed interface.

Discussion: 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.

(17) BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS

Enforce adherence to protocol formats.

Discussion: System components that enforce protocol formats include deep packet inspection firewalls and XML gateways. The components verify adherence to protocol

formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.

Related Controls: SC-4.

(18) BOUNDARY PROTECTION | FAIL SECURE

Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

Discussion: 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.

(19) BOUNDARY PROTECTION | BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS

Block inbound and outbound communications traffic between [*Assignment: organization-defined communication clients*] that are independently configured by end users and external service providers.

Discussion: Communication clients independently configured by end users and external service providers include instant messaging clients and video conferencing software and applications. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.

Related Controls: None.

(20) BOUNDARY PROTECTION | DYNAMIC ISOLATION AND SEGREGATION

Provide the capability to dynamically isolate [*Assignment: organization-defined system components*] from other system components.

Discussion: The capability to dynamically isolate certain internal system components is useful when it is necessary to partition or separate system components of questionable origin from components that possess greater trustworthiness. Component isolation reduces the attack surface of organizational systems. Isolating selected system components can also limit the damage from successful attacks when such attacks occur.

Related Controls: None.

(21) BOUNDARY PROTECTION | ISOLATION OF SYSTEM COMPONENTS

Employ boundary protection mechanisms to isolate [*Assignment: organization-defined system components*] supporting [*Assignment: organization-defined missions and/or business functions*].

Discussion: 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.

(22) BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS

Implement separate network addresses to connect to systems in different security domains.

Discussion: The decomposition of systems into subnetworks (i.e., subnets) helps to provide the appropriate level of protection for network connections to different security domains that contain information with different security categories or classification levels.

Related Controls: None.

(23) BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE

Disable feedback to senders on protocol format validation failure.

Discussion: Disabling feedback to senders when there is a failure in protocol validation format prevents adversaries from obtaining information that would otherwise be unavailable.

Related Controls: None.

(24) BOUNDARY PROTECTION | PERSONALLY IDENTIFIABLE INFORMATION

For systems that process personally identifiable information:

(a) Apply the following processing rules to data elements of personally identifiable information: [*Assignment: organization-defined processing rules*];

(b) Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;

(c) Document each processing exception; and

(d) Review and remove exceptions that are no longer supported.

Discussion: Managing the processing of personally identifiable information is an important aspect of protecting an individual's privacy. Applying, monitoring for, and documenting exceptions to processing rules ensure that personally identifiable information is processed only in accordance with established privacy requirements.

Related Controls: PT-2, SI-15.

(25) BOUNDARY PROTECTION | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

Prohibit the direct connection of [*Assignment: organization-defined unclassified national security system*] to an external network without the use of [*Assignment: organization-defined boundary protection device*].

Discussion: A direct connection is a dedicated physical or virtual connection between two or more systems. Organizations typically do not have complete control over external networks, including the Internet. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between unclassified national security systems and external networks.

Related Controls: None.

(26) BOUNDARY PROTECTION | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

Prohibit the direct connection of a classified national security system to an external network without the use of [*Assignment: organization-defined boundary protection device*].

Discussion: A direct connection is a dedicated physical or virtual connection between two or more systems. Organizations typically do not have complete control over external networks,

including the Internet. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between classified national security systems and external networks. In addition, approved boundary protection devices (typically managed interface or cross-domain systems) provide information flow enforcement from systems to external networks.

Related Controls: None.

(27) BOUNDARY PROTECTION | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS

Prohibit the direct connection of [*Assignment: organization-defined unclassified non-national security system*] to an external network without the use of [*Assignment: organization-defined boundary protection device*].

Discussion: A direct connection is a dedicated physical or virtual connection between two or more systems. Organizations typically do not have complete control over external networks, including the Internet. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between unclassified non-national security systems and external networks.

Related Controls: None.

(28) BOUNDARY PROTECTION | CONNECTIONS TO PUBLIC NETWORKS

Prohibit the direct connection of [*Assignment: organization-defined system*] to a public network.

Discussion: 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.

(29) BOUNDARY PROTECTION | SEPARATE SUBNETS TO ISOLATE FUNCTIONS

Implement [*Selection: physically; logically*] separate subnetworks to isolate the following critical system components and functions: [*Assignment: organization-defined critical system components and functions*].

Discussion: 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.

References: [OMB A-130], [FIPS 199], [SP 800-37], [SP 800-41], [SP 800-77], [SP 800-189].

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control: Protect the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

Discussion: 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.

Control Enhancements:

(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to [*Selection (one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission.

Discussion: 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.

(2) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE- AND POST-TRANSMISSION HANDLING

Maintain the [*Selection (one or more): confidentiality; integrity*] of information during preparation for transmission and during reception.

Discussion: Information can be unintentionally or maliciously disclosed or modified during preparation for transmission or during reception, including during aggregation, at protocol transformation points, and during packing and unpacking. Such unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Related Controls: None.

(3) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS

Implement cryptographic mechanisms to protect message externals unless otherwise protected by [*Assignment: organization-defined alternative physical controls*].

Discussion: Cryptographic protection for message externals addresses protection from the unauthorized disclosure of information. Message externals include message headers and routing information. Cryptographic protection prevents the exploitation of message externals and applies to internal and external networks or links that may be visible to individuals who are not authorized users. Header and routing information is sometimes transmitted in clear text (i.e., unencrypted) because the information is not identified by organizations as having significant value or because encrypting the information can result in lower network performance or higher costs. Alternative physical controls include protected distribution systems.

Related Controls: SC-12, SC-13.

(4) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL OR RANDOMIZE COMMUNICATIONS

Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [*Assignment: organization-defined alternative physical controls*].

Discussion: Concealing or randomizing communication patterns addresses protection from unauthorized disclosure of information. Communication patterns include frequency, periods, predictability, and amount. Changes to communications patterns can reveal information with intelligence value, especially when combined with other available information related to the mission and business functions of the organization. Concealing or randomizing communications prevents the derivation of intelligence based on communications patterns and applies to both internal and external networks or links that may be visible to individuals who are not authorized users. Encrypting the links and transmitting in continuous, fixed, or random patterns prevents the derivation of intelligence from the system communications patterns. Alternative physical controls include protected distribution systems.

Related Controls: SC-12, SC-13.

(5) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PROTECTED DISTRIBUTION SYSTEM

Implement [*Assignment: organization-defined protected distribution system*] to [*Selection (one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission.

Discussion: The purpose of a protected distribution system is to deter, detect, and/or make difficult physical access to the communication lines that carry national security information.

Related Controls: None.

References: [FIPS 140-3], [FIPS 197], [SP 800-52], [SP 800-77], [SP 800-81-2], [SP 800-113], [SP 800-177], [IR 8023].

SC-9 TRANSMISSION CONFIDENTIALITY

[Withdrawn: Incorporated into SC-8.]

SC-10 NETWORK DISCONNECT

Control: Terminate the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.

Discussion: Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

Related Controls: AC-17, SC-23.

Control Enhancements: None.

References: None.

SC-11 TRUSTED PATH

Control:

a. Provide a [*Selection: physically; logically*] isolated trusted communications path for communications between the user and the trusted components of the system; and

b. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: [*Assignment: organization-defined security functions*].

Discussion: Trusted paths are mechanisms by which users can communicate (using input devices such as keyboards) directly with the security functions of systems with the requisite assurance to support security policies. Trusted path mechanisms can only be activated by users or the security functions of organizational systems. User responses that occur via trusted paths are protected from modification by and disclosure to untrusted applications. Organizations employ trusted paths for trustworthy, high-assurance connections between security functions of systems and users, including during system logons. The original implementations of trusted paths employed an out-of-band signal to initiate the path, such as using the <BREAK> key, which does not transmit characters that can be spoofed. In later implementations, a key combination that could not be hijacked was used (e.g., the <CTRL> + <ALT> + <DEL> keys). Such key combinations, however, are platform-specific and may not provide a trusted path implementation in every case. The enforcement of trusted communications paths is provided by a specific implementation that meets the reference monitor concept.

Related Controls: AC-16, AC-25, SC-12, SC-23.

Control Enhancements:

(1) TRUSTED PATH | IRREFUTABLE COMMUNICATIONS PATH

(a) Provide a trusted communications path that is irrefutably distinguishable from other communications paths; and

(b) Initiate the trusted communications path for communications between the [*Assignment: organization-defined security functions*] of the system and the user.

Discussion: An irrefutable communications path permits the system to initiate a trusted path, which necessitates that the user can unmistakably recognize the source of the communication as a trusted system component. For example, the trusted path may appear in an area of the display that other applications cannot access or be based on the presence of an identifier that cannot be spoofed.

Related Controls: None.

References: [OMB A-130].

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

Discussion: 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.

Control Enhancements:

(1) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY

Maintain availability of information in the event of the loss of cryptographic keys by users.

Discussion: 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.

(2) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS

Produce, control, and distribute symmetric cryptographic keys using [*Selection: NIST FIPS-validated; NSA-approved*] key management technology and processes.

Discussion: [SP 800-56A], [SP 800-56B], and [SP 800-56C] provide guidance on cryptographic key establishment schemes and key derivation methods. [SP 800-57-1], [SP 800-57-2], and [SP 800-57-3] provide guidance on cryptographic key management.

Related Controls: None.

(3) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS

Produce, control, and distribute asymmetric cryptographic keys using [*Selection: NSA-approved key management technology and processes; prepositioned keying material; DoD-approved or DoD-issued Medium Assurance PKI certificates; DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with organization-defined requirements*].

Discussion: [SP 800-56A], [SP 800-56B], and [SP 800-56C] provide guidance on cryptographic key establishment schemes and key derivation methods. [SP 800-57-1], [SP 800-57-2], and [SP 800-57-3] provide guidance on cryptographic key management.

Related Controls: None.

(4) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES

[Withdrawn: Incorporated into SC-12(3).]

(5) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS

[Withdrawn: Incorporated into SC-12(3).]

(6) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PHYSICAL CONTROL OF KEYS

Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.

Discussion: For organizations that use external service providers (e.g., cloud service or data center providers), physical control of cryptographic keys provides additional assurance that information stored by such external providers is not subject to unauthorized disclosure or modification.

Related Controls: None.

References: [FIPS 140-3], [SP 800-56A], [SP 800-56B], [SP 800-56C], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-63-3], [IR 7956], [IR 7966].

SC-13 CRYPTOGRAPHIC PROTECTION

Control:

a. Determine the [*Assignment: organization-defined cryptographic uses*]; and

b. Implement the following types of cryptography required for each specified cryptographic use: [*Assignment: organization-defined types of cryptography for each specified cryptographic use*].

Discussion: 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.

Control Enhancements: None.

(1) CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY

[Withdrawn: Incorporated into SC-13.]

(2) CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY

[Withdrawn: Incorporated into SC-13.]

(3) CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS

[Withdrawn: Incorporated into SC-13.]

(4) CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES

[Withdrawn: Incorporated into SC-13.]

References: [FIPS 140-3].

SC-14 PUBLIC ACCESS PROTECTIONS

[Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, and SI-10.]

SC-15 COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

Control:

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and

b. Provide an explicit indication of use to users physically present at the devices.

Discussion: 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.

Control Enhancements:

(1) COLLABORATIVE COMPUTING DEVICES | PHYSICAL OR LOGICAL DISCONNECT

Provide [*Selection (one or more): physical; logical*] disconnect of collaborative computing devices in a manner that supports ease of use.

Discussion: Failing to disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to disconnect from such devices after a collaborative computing session ensures that participants carry out the disconnect activity without having to go through complex and tedious procedures. Disconnect from collaborative computing devices can be manual or automatic.

Related Controls: None.

(2) COLLABORATIVE COMPUTING DEVICES | BLOCKING INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

[Withdrawn: Incorporated into SC-7.]

(3) COLLABORATIVE COMPUTING DEVICES | DISABLING AND REMOVAL IN SECURE WORK AREAS

Disable or remove collaborative computing devices and applications from [*Assignment: organization-defined systems or system components*] in [*Assignment: organization-defined secure work areas*].

Discussion: Failing to disable or remove collaborative computing devices and applications from systems or system components can result in compromises of information, including eavesdropping on conversations. A Sensitive Compartmented Information Facility (SCIF) is an example of a secure work area.

Related Controls: None.

(4) COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS

Provide an explicit indication of current participants in [*Assignment: organization-defined online meetings and teleconferences*].

Discussion: Explicitly indicating current participants prevents unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.

Related Controls: None.

References: None.

SC-16 TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES

Control: Associate [*Assignment: organization-defined security and privacy attributes*] with information exchanged between systems and between system components.

Discussion: Security and privacy attributes can be explicitly or implicitly associated with the information contained in organizational systems or system components. Attributes are abstractions that represent the basic properties or characteristics of an entity with respect to protecting information or the management of personally identifiable information. Attributes are typically associated with internal data structures, including records, buffers, and files within the system. Security and privacy attributes are used to implement access control and information flow control policies; reflect special dissemination, management, or distribution instructions, including permitted uses of personally identifiable information; or support other aspects of the information security and privacy policies. Privacy attributes may be used independently or in conjunction with security attributes.

Related Controls: AC-3, AC-4, AC-16.

Control Enhancements:

(1) TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES | INTEGRITY VERIFICATION

Verify the integrity of transmitted security and privacy attributes.

Discussion: Part of verifying the integrity of transmitted information is ensuring that security and privacy attributes that are associated with such information have not been modified in an unauthorized manner. Unauthorized modification of security or privacy attributes can result in a loss of integrity for transmitted information.

Related Controls: AU-10, SC-8.

(2) TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES | ANTI-SPOOFING MECHANISMS

Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process.

Discussion: Some attack vectors operate by altering the security attributes of an information system to intentionally and maliciously implement an insufficient level of security within the system. The alteration of attributes leads organizations to believe that a greater number of security functions are in place and operational than have actually been implemented.

Related Controls: SI-3, SI-4, SI-7.

(3) TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES | CRYPTOGRAPHIC BINDING

Implement [*Assignment: organization-defined mechanisms or techniques*] to bind security and privacy attributes to transmitted information.

Discussion: Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of such information.

Related Controls: AC-16, SC-12, SC-13.

References: [OMB A-130].

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control:

a. Issue public key certificates under an [*Assignment: organization-defined certificate policy*] or obtain public key certificates from an approved service provider; and

b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

Discussion: 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.

Control Enhancements: None.

References: [SP 800-32], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-63-3].

SC-18 MOBILE CODE

Control:

a. Define acceptable and unacceptable mobile code and mobile code technologies; and

b. Authorize, monitor, and control the use of mobile code within the system.

Discussion: 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.

Control Enhancements:

(1) MOBILE CODE | IDENTIFY UNACCEPTABLE CODE AND TAKE CORRECTIVE ACTIONS

Identify [*Assignment: organization-defined unacceptable mobile code*] and take [*Assignment: organization-defined corrective actions*].

Discussion: Corrective actions when unacceptable mobile code is detected include blocking, quarantine, or alerting administrators. Blocking includes preventing the transmission of word processing files with embedded macros when such macros have been determined to be unacceptable mobile code.

Related Controls: None.

(2) MOBILE CODE | ACQUISITION, DEVELOPMENT, AND USE

Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [*Assignment: organization-defined mobile code requirements*].

Discussion: None.

Related Controls: None.

(3) MOBILE CODE | PREVENT DOWNLOADING AND EXECUTION

Prevent the download and execution of [*Assignment: organization-defined unacceptable mobile code*].

Discussion: None.

Related Controls: None.

(4) MOBILE CODE | PREVENT AUTOMATIC EXECUTION

Prevent the automatic execution of mobile code in [*Assignment: organization-defined software applications*] and enforce [*Assignment: organization-defined actions*] prior to executing the code.

Discussion: Actions enforced before executing mobile code include prompting users prior to opening email attachments or clicking on web links. Preventing the automatic execution of mobile code includes disabling auto-execute features on system components that employ portable storage devices, such as compact discs, digital versatile discs, and universal serial bus devices.

Related Controls: None.

(5) MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS

Allow execution of permitted mobile code only in confined virtual machine environments.

Discussion: Permitting the execution of mobile code only in confined virtual machine environments helps prevent the introduction of malicious code into other systems and system components.

Related Controls: SC-44, SI-7.

References: [SP 800-28].

SC-19 VOICE OVER INTERNET PROTOCOL

[Withdrawn: Technology-specific; addressed as any other technology or protocol.]

SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control:

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Discussion: 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.

Control Enhancements:

(1) SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES

[Withdrawn: Incorporated into SC-20.]

(2) SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN AND INTEGRITY

Provide data origin and integrity protection artifacts for internal name/address resolution queries.

Discussion: None.

Related Controls: None.

References: [FIPS 140-3], [FIPS 186-4], [SP 800-81-2].

SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Control: Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Discussion: 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.

Control Enhancements: None.

(1) SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | DATA ORIGIN AND INTEGRITY

[Withdrawn: Incorporated into SC-21.]

References: [SP 800-81-2].

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

Control: Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Discussion: 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.

Control Enhancements: None.

References: [SP 800-81-2].

SC-23 SESSION AUTHENTICITY

Control: Protect the authenticity of communications sessions.

Discussion: 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.

Control Enhancements:

(1) SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT

Invalidate session identifiers upon user logout or other session termination.

Discussion: Invalidating session identifiers at logout curtails the ability of adversaries to capture and continue to employ previously valid session IDs.

Related Controls: None.

(2) SESSION AUTHENTICITY | USER-INITIATED LOGOUTS AND MESSAGE DISPLAYS

[Withdrawn: Incorporated into AC-12(1).]

(3) SESSION AUTHENTICITY | UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS

Generate a unique session identifier for each session with [*Assignment: organization-defined randomness requirements*] and recognize only session identifiers that are system-generated.

Discussion: Generating unique session identifiers curtails the ability of adversaries to reuse previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.

Related Controls: AC-10, SC-12, SC-13.

(4) SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION

[Withdrawn: Incorporated into SC-23(3).]

(5) SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES

Only allow the use of [*Assignment: organization-defined certificate authorities*] for verification of the establishment of protected sessions.

Discussion: Reliance on certificate authorities for the establishment of secure sessions includes the use of Transport Layer Security (TLS) certificates. These certificates, after verification by their respective certificate authorities, facilitate the establishment of protected sessions between web clients and web servers.

Related Controls: SC-12, SC-13.

References: [SP 800-52], [SP 800-77], [SP 800-95], [SP 800-113].

SC-24 FAIL IN KNOWN STATE

Control: Fail to a [*Assignment: organization-defined known system state*] for the following failures on the indicated components while preserving [*Assignment: organization-defined system state information*] in failure: [*Assignment: list of organization-defined types of system failures on organization-defined system components*].

Discussion: 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.

Control Enhancements: None.

References: None.

SC-25 THIN NODES

Control: Employ minimal functionality and information storage on the following system components: [*Assignment: organization-defined system components*].

Discussion: The deployment of system components with minimal functionality reduces the need to secure every endpoint and may reduce the exposure of information, systems, and services to attacks. Reduced or minimal functionality includes diskless nodes and thin client technologies.

Related Controls: SC-30, SC-44.

Control Enhancements: None.

References: None.

SC-26 DECOYS

Control: Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.

Discussion: Decoys (i.e., honeypots, honeynets, or deception nets) are established to attract adversaries and deflect attacks away from the operational systems that support organizational mission and business functions. Use of decoys requires some supporting isolation measures to ensure that any deflected malicious code does not infect organizational systems. Depending on the specific usage of the decoy, consultation with the Office of the General Counsel before deployment may be needed.

Related Controls: RA-5, SC-7, SC-30, SC-35, SC-44, SI-3, SI-4.

Control Enhancements: None.

(1) DECOYS | DETECTION OF MALICIOUS CODE

[Withdrawn: Incorporated into SC-35.]

References: None.

SC-27 PLATFORM-INDEPENDENT APPLICATIONS

Control: Include within organizational systems the following platform independent applications: [*Assignment: organization-defined platform-independent applications*].

Discussion: Platforms are combinations of hardware, firmware, and software components used to execute software applications. Platforms include operating systems, the underlying computer architectures, or both. Platform-independent applications are applications with the capability to execute on multiple platforms. Such applications promote portability and reconstitution on different platforms. Application portability and the ability to reconstitute on different platforms increase the availability of mission-essential functions within organizations in situations where systems with specific operating systems are under attack.

Related Controls: SC-29.

Control Enhancements: None.

References: None.

SC-28 PROTECTION OF INFORMATION AT REST

Control: Protect the [*Selection (one or more): confidentiality; integrity*] of the following information at rest: [*Assignment: organization-defined information at rest*].

Discussion: 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.

Control Enhancements:

(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [*Assignment: organization-defined system components or media*]: [*Assignment: organization-defined information*].

Discussion: 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.

(2) PROTECTION OF INFORMATION AT REST | OFFLINE STORAGE

Remove the following information from online storage and store offline in a secure location: [*Assignment: organization-defined information*].

Discussion: Removing organizational information from online storage to offline storage eliminates the possibility of individuals gaining unauthorized access to the information through a network. Therefore, organizations may choose to move information to offline storage in lieu of protecting such information in online storage.

Related Controls: None.

(3) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC KEYS

Provide protected storage for cryptographic keys [*Selection:* [*Assignment: organization-defined safeguards*]; *hardware-protected key store*].

Discussion: A Trusted Platform Module (TPM) is an example of a hardware-protected data store that can be used to protect cryptographic keys.

Related Controls: SC-12, SC-13.

References: [OMB A-130], [SP 800-56A], [SP 800-56B], [SP 800-56C], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-111], [SP 800-124].

SC-29 HETEROGENEITY

Control: Employ a diverse set of information technologies for the following system components in the implementation of the system: [*Assignment: organization-defined system components*].

Discussion: 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.

Control Enhancements:

(1) HETEROGENEITY | VIRTUALIZATION TECHNIQUES

Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [*Assignment: organization-defined frequency*].

Discussion: While frequent changes to operating systems and applications can pose significant configuration management challenges, the changes can result in an increased work factor for adversaries to conduct successful attacks. Changing virtual operating systems or applications, as opposed to changing actual operating systems or applications, provides virtual changes that impede attacker success while reducing configuration management efforts. Virtualization techniques can assist in isolating untrustworthy software or software of dubious provenance into confined execution environments.

Related Controls: None.

References: None.

SC-30 CONCEALMENT AND MISDIRECTION

Control: Employ the following concealment and misdirection techniques for [*Assignment: organization-defined systems*] at [*Assignment: organization-defined time periods*] to confuse and mislead adversaries: [*Assignment: organization-defined concealment and misdirection techniques*].

Discussion: 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.

Control Enhancements:

(1) CONCEALMENT AND MISDIRECTION | VIRTUALIZATION TECHNIQUES

[Withdrawn: Incorporated into SC-29(1).]

(2) CONCEALMENT AND MISDIRECTION | RANDOMNESS

Employ [*Assignment: organization-defined techniques*] to introduce randomness into organizational operations and assets.

Discussion: Randomness introduces increased levels of uncertainty for adversaries regarding the actions that organizations take to defend their systems against attacks. Such actions may impede the ability of adversaries to correctly target information resources of organizations that support critical missions or business functions. Uncertainty may also cause adversaries to hesitate before initiating or continuing attacks. Misdirection techniques that involve

randomness include performing certain routine actions at different times of day, employing different information technologies, using different suppliers, and rotating roles and responsibilities of organizational personnel.

Related Controls: None.

(3) CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING AND STORAGE LOCATIONS

Change the location of [*Assignment: organization-defined processing and/or storage*] [*Selection:* [*Assignment: organization-defined time frequency*]*; at random time intervals*]].

Discussion: Adversaries target critical mission and business functions and the systems that support those mission and business functions while also trying to minimize the exposure of their existence and tradecraft. The static, homogeneous, and deterministic nature of organizational systems targeted by adversaries make such systems more susceptible to attacks with less adversary cost and effort to be successful. Changing processing and storage locations (also referred to as moving target defense) addresses the advanced persistent threat using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the system components (i.e., processing, storage) that support critical mission and business functions. Changing the locations of processing activities and/or storage sites introduces a degree of uncertainty into the targeting activities of adversaries. The targeting uncertainty increases the work factor of adversaries and makes compromises or breaches of the organizational systems more difficult and time-consuming. It also increases the chances that adversaries may inadvertently disclose certain aspects of their tradecraft while attempting to locate critical organizational resources.

Related Controls: None.

(4) CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION

Employ realistic, but misleading information in [*Assignment: organization-defined system components*] about its security state or posture.

Discussion: Employing misleading information is intended to confuse potential adversaries regarding the nature and extent of controls deployed by organizations. Thus, adversaries may employ incorrect and ineffective attack techniques. One technique for misleading adversaries is for organizations to place misleading information regarding the specific controls deployed in external systems that are known to be targeted by adversaries. Another technique is the use of deception nets that mimic actual aspects of organizational systems but use, for example, out-of-date software configurations.

Related Controls: None.

(5) CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS

Employ the following techniques to hide or conceal [*Assignment: organization-defined system components*]: [*Assignment: organization-defined techniques*].

Discussion: By hiding, disguising, or concealing critical system components, organizations may be able to decrease the probability that adversaries target and successfully compromise those assets. Potential means to hide, disguise, or conceal system components include the configuration of routers or the use of encryption or virtualization techniques.

Related Controls: None.

References: None.

SC-31 COVERT CHANNEL ANALYSIS

Control:

a. Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert [*Selection (one or more): storage; timing*] channels; and

b. Estimate the maximum bandwidth of those channels.

Discussion: 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.

Control Enhancements:

(1) COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY

Test a subset of the identified covert channels to determine the channels that are exploitable.

Discussion: None.

Related Controls: None.

(2) COVERT CHANNEL ANALYSIS | MAXIMUM BANDWIDTH

Reduce the maximum bandwidth for identified covert [*Selection (one or more): storage; timing*] channels to [*Assignment: organization-defined values*].

Discussion: The complete elimination of covert channels, especially covert timing channels, is usually not possible without significant performance impacts.

Related Controls: None.

(3) COVERT CHANNEL ANALYSIS | MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS

Measure the bandwidth of [*Assignment: organization-defined subset of identified covert channels*] in the operational environment of the system.

Discussion: Measuring covert channel bandwidth in specified operational environments helps organizations determine how much information can be covertly leaked before such leakage adversely affects mission or business functions. Covert channel bandwidth may be significantly different when measured in settings that are independent of the specific environments of operation, including laboratories or system development environments.

Related Controls: None.

References: None.

SC-32 SYSTEM PARTITIONING

Control: Partition the system into [*Assignment: organization-defined system components*] residing in separate [*Selection: physical; logical*] domains or environments based on [*Assignment: organization-defined circumstances for physical or logical separation of components*].

Discussion: System partitioning is part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components. Physical separation options include physically distinct components in separate racks in the same room, critical components in separate rooms, and geographical separation of critical components. Security categorization can guide the selection of candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned system components.

Related Controls: AC-4, AC-6, SA-8, SC-2, SC-3, SC-7, SC-36.

Control Enhancements:

(1) SYSTEM PARTITIONING | SEPARATE PHYSICAL DOMAINS FOR PRIVILEGED FUNCTIONS

Partition privileged functions into separate physical domains.

Discussion: Privileged functions that operate in a single physical domain may represent a single point of failure if that domain becomes compromised or experiences a denial of service.

Related Controls: None.

References: [FIPS 199], [IR 8179].

SC-33 TRANSMISSION PREPARATION INTEGRITY

[Withdrawn: Incorporated into SC-8.]

SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS

Control: For [*Assignment: organization-defined system components*], load and execute:

a. The operating environment from hardware-enforced, read-only media; and

b. The following applications from hardware-enforced, read-only media: [*Assignment: organization-defined applications*].

Discussion: The operating environment for a system contains the code that hosts applications, including operating systems, executives, or virtual machine monitors (i.e., hypervisors). It can also include certain applications that run directly on hardware platforms. Hardware-enforced, read-only media include Compact Disc-Recordable (CD-R) and Digital Versatile Disc-Recordable (DVD-R) disk drives as well as one-time, programmable, read-only memory. The use of non-modifiable storage ensures the integrity of software from the point of creation of the read-only image. The use of reprogrammable, read-only memory can be accepted as read-only media provided that integrity can be adequately protected from the point of initial writing to the insertion of the memory into the system, and there are reliable hardware protections against reprogramming the memory while installed in organizational systems.

Related Controls: AC-3, SI-7, SI-14.

Control Enhancements:

(1) NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE

Employ [*Assignment: organization-defined system components*] with no writeable storage that is persistent across component restart or power on/off.

Discussion: Disallowing writeable storage eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated system components. The restriction applies to fixed and removable storage, with the latter being addressed either directly or as specific restrictions imposed through access controls for mobile devices.

Related Controls: AC-19, MP-7.

(2) NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION ON READ-ONLY MEDIA

Protect the integrity of information prior to storage on read-only media and control the media after such information has been recorded onto the media.

Discussion: Controls prevent the substitution of media into systems or the reprogramming of programmable read-only media prior to installation into the systems. Integrity protection controls include a combination of prevention, detection, and response.

Related Controls: CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SC-28, SI-3.

(3) NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION

[Withdrawn: Moved to SC-51.]

SC-35 EXTERNAL MALICIOUS CODE IDENTIFICATION

Control: Include system components that proactively seek to identify network-based malicious code or malicious websites.

Discussion: External malicious code identification differs from decoys in SC-26 in that the components actively probe networks, including the Internet, in search of malicious code contained on external websites. Like decoys, the use of external malicious code identification techniques requires some supporting isolation measures to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational systems. Virtualization is a common technique for achieving such isolation.

Related Controls: SC-7, SC-26, SC-44, SI-3, SI-4.

Control Enhancements: None.

References: None.

SC-36 DISTRIBUTED PROCESSING AND STORAGE

Control: Distribute the following processing and storage components across multiple [*Selection: physical locations; logical domains*]: [*Assignment: organization-defined processing and storage components*].

Discussion: Distributing processing and storage across multiple physical locations or logical domains provides a degree of redundancy or overlap for organizations. The redundancy and overlap increase the work factor of adversaries to adversely impact organizational operations, assets, and individuals. The use of distributed processing and storage does not assume a single primary processing or storage location. Therefore, it allows for parallel processing and storage.

Related Controls: CP-6, CP-7, PL-8, SC-32.

Control Enhancements:

(1) DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES

(a) Employ polling techniques to identify potential faults, errors, or compromises to the following processing and storage components: [*Assignment: organization-defined distributed processing and storage components*]; and

(b) Take the following actions in response to identified faults, errors, or compromises: [*Assignment: organization-defined actions*].

Discussion: Distributed processing and/or storage may be used to reduce opportunities for adversaries to compromise the confidentiality, integrity, or availability of organizational information and systems. However, the distribution of processing and storage components does not prevent adversaries from compromising one or more of the components. Polling compares the processing results and/or storage content from the distributed components and subsequently votes on the outcomes. Polling identifies potential faults, compromises, or errors in the distributed processing and storage components.

Related Controls: SI-4.

(2) DISTRIBUTED PROCESSING AND STORAGE | SYNCHRONIZATION

Synchronize the following duplicate systems or system components: [*Assignment: organization-defined duplicate systems or system components*].

Discussion: SC-36 and CP-9(6) require the duplication of systems or system components in distributed locations. The synchronization of duplicated and redundant services and data helps to ensure that information contained in the distributed locations can be used in the mission or business functions of organizations, as needed.

Related Controls: CP-9.

References: [SP 800-160-2].

SC-37 OUT-OF-BAND CHANNELS

Control: Employ the following out-of-band channels for the physical delivery or electronic transmission of [*Assignment: organization-defined information, system components, or devices*] to [*Assignment: organization-defined individuals or systems*]: [*Assignment: organization-defined out-of-band channels*].

Discussion: Out-of-band channels include local, non-network accesses to systems; network paths physically separate from network paths used for operational traffic; or non-electronic paths, such as the U.S. Postal Service. The use of out-of-band channels is contrasted with the use of in-band channels (i.e., the same channels) that carry routine operational traffic. Out-of-band channels do not have the same vulnerability or exposure as in-band channels. Therefore, the confidentiality, integrity, or availability compromises of in-band channels will not compromise or adversely affect the out-of-band channels. Organizations may employ out-of-band channels in the delivery or transmission of organizational items, including authenticators and credentials; cryptographic key management information; system and data backups; configuration management changes for hardware, firmware, or software; security updates; maintenance information; and malicious code protection updates.

Related Controls: AC-2, CM-3, CM-5, CM-7, IA-2, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.

Control Enhancements:

(1) OUT-OF-BAND CHANNELS | ENSURE DELIVERY AND TRANSMISSION

Employ [*Assignment: organization-defined controls*] to ensure that only [*Assignment: organization-defined individuals or systems*] receive the following information, system components, or devices: [*Assignment: organization-defined information, system components, or devices*].

Discussion: Techniques employed by organizations to ensure that only designated systems or individuals receive certain information, system components, or devices include sending authenticators via an approved courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.

Related Controls: None.

References: [SP 800-57-1], [SP 800-57-2], [SP 800-57-3].

SC-38 OPERATIONS SECURITY

Control: Employ the following operations security controls to protect key organizational information throughout the system development life cycle: [*Assignment: organization-defined operations security controls*].

Discussion: Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and the application of appropriate countermeasures. OPSEC controls are

applied to organizational systems and the environments in which those systems operate. OPSEC controls protect the confidentiality of information, including limiting the sharing of information with suppliers, potential suppliers, and other non-organizational elements and individuals. Information critical to organizational mission and business functions includes user identities, element uses, suppliers, supply chain processes, functional requirements, security requirements, system design specifications, testing and evaluation protocols, and security control implementation details.

Related Controls: CA-2, CA-7, PL-1, PM-9, PM-12, RA-2, RA-3, RA-5, SC-7, SR-3, SR-7.

Control Enhancements: None.

References: None.

SC-39 PROCESS ISOLATION

Control: Maintain a separate execution domain for each executing system process.

Discussion: 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.

Control Enhancements:

(1) PROCESS ISOLATION | HARDWARE SEPARATION

Implement hardware separation mechanisms to facilitate process isolation.

Discussion: Hardware-based separation of system processes is generally less susceptible to compromise than software-based separation, thus providing greater assurance that the separation will be enforced. Hardware separation mechanisms include hardware memory management.

Related Controls: None.

(2) PROCESS ISOLATION | SEPARATE EXECUTION DOMAIN PER THREAD

Maintain a separate execution domain for each thread in [*Assignment: organization-defined multi-threaded processing*].

Discussion: None.

Related Controls: None.

References: [SP 800-160-1].

SC-40 WIRELESS LINK PROTECTION

Control: Protect external and internal [*Assignment: organization-defined wireless links*] from the following signal parameter attacks: [*Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks*].

Discussion: Wireless link protection applies to internal and external wireless communication links that may be visible to individuals who are not authorized system users. Adversaries can

exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or spoof system users. Protection of wireless links reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may not be possible to implement wireless link protections to the extent necessary to meet organizational security requirements.

Related Controls: AC-18, SC-5.

Control Enhancements:

(1) WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE

Implement cryptographic mechanisms that achieve [*Assignment: organization-defined level of protection*] against the effects of intentional electromagnetic interference.

Discussion: The implementation of cryptographic mechanisms for electromagnetic interference protects systems against intentional jamming that might deny or impair communications by ensuring that wireless spread spectrum waveforms used to provide anti-jam protection are not predictable by unauthorized individuals. The implementation of cryptographic mechanisms may also coincidentally mitigate the effects of unintentional jamming due to interference from legitimate transmitters that share the same spectrum. Mission requirements, projected threats, concept of operations, and laws, executive orders, directives, regulations, policies, and standards determine levels of wireless link availability, cryptography needed, and performance.

Related Controls: PE-21, SC-12, SC-13.

(2) WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL

Implement cryptographic mechanisms to reduce the detection potential of wireless links to [*Assignment: organization-defined level of reduction*].

Discussion: The implementation of cryptographic mechanisms to reduce detection potential is used for covert communications and to protect wireless transmitters from geo-location. It also ensures that the spread spectrum waveforms used to achieve a low probability of detection are not predictable by unauthorized individuals. Mission requirements, projected threats, concept of operations, and applicable laws, executive orders, directives, regulations, policies, and standards determine the levels to which wireless links are undetectable.

Related Controls: SC-12, SC-13.

(3) WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION

Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.

Discussion: The implementation of cryptographic mechanisms to identify and reject imitative or manipulative communications ensures that the signal parameters of wireless transmissions are not predictable by unauthorized individuals. Such unpredictability reduces the probability of imitative or manipulative communications deception based on signal parameters alone.

Related Controls: SC-12, SC-13, SI-4.

(4) WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION

Implement cryptographic mechanisms to prevent the identification of [*Assignment: organization-defined wireless transmitters*] by using the transmitter signal parameters.

Discussion: The implementation of cryptographic mechanisms to prevent the identification of wireless transmitters protects against the unique identification of wireless transmitters

for the purposes of intelligence exploitation by ensuring that anti-fingerprinting alterations to signal parameters are not predictable by unauthorized individuals. It also provides anonymity when required. Radio fingerprinting techniques identify the unique signal parameters of transmitters to fingerprint such transmitters for purposes of tracking and mission or user identification.

Related Controls: SC-12, SC-13.

References: None.

SC-41 PORT AND I/O DEVICE ACCESS

Control: [*Selection: Physically; Logically*] disable or remove [*Assignment: organization-defined connection ports or input/output devices*] on the following systems or system components: [*Assignment: organization-defined systems or system components*].

Discussion: 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.

Control Enhancements: None.

References: None.

SC-42 SENSOR CAPABILITY AND DATA

Control:

a. Prohibit [*Selection (one or more): the use of devices possessing* [*Assignment: organization-defined environmental sensing capabilities*] *in* [*Assignment: organization-defined facilities, areas, or systems*]; *the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions:* [*Assignment: organization-defined exceptions where remote activation of sensors is allowed*]]; and

b. Provide an explicit indication of sensor use to [*Assignment: organization-defined group of users*].

Discussion: Sensor capability and data applies to types of systems or system components characterized as mobile devices, such as cellular telephones, smart phones, and tablets. Mobile devices often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include microphones, cameras, Global Positioning System (GPS) mechanisms, and accelerometers. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the movements of an individual. Organizations may prohibit individuals from bringing cellular telephones or digital cameras into certain designated facilities or controlled areas within facilities where classified information is stored or sensitive conversations are taking place.

Related Controls: SC-15.

Control Enhancements:

(1) SENSOR CAPABILITY AND DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES

Verify that the system is configured so that data or information collected by the [*Assignment: organization-defined sensors*] is only reported to authorized individuals or roles.

Discussion: In situations where sensors are activated by authorized individuals, it is still possible that the data or information collected by the sensors will be sent to unauthorized entities.

Related Controls: None.

(2) SENSOR CAPABILITY AND DATA | AUTHORIZED USE

Employ the following measures so that data or information collected by [*Assignment: organization-defined sensors*] is only used for authorized purposes: [*Assignment: organization-defined measures*].

Discussion: Information collected by sensors for a specific authorized purpose could be misused for some unauthorized purpose. For example, GPS sensors that are used to support traffic navigation could be misused to track the movements of individuals. Measures to mitigate such activities include additional training to help ensure that authorized individuals do not abuse their authority and, in the case where sensor data is maintained by external parties, contractual restrictions on the use of such data.

Related Controls: PT-2.

(3) SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES

[Withdrawn: Incorporated into SC-42.]

(4) SENSOR CAPABILITY AND DATA | NOTICE OF COLLECTION

Employ the following measures to facilitate an individual's awareness that personally identifiable information is being collected by [*Assignment: organization-defined sensors*]: [*Assignment: organization-defined measures*].

Discussion: Awareness that organizational sensors are collecting data enables individuals to more effectively engage in managing their privacy. Measures can include conventional written notices and sensor configurations that make individuals directly or indirectly aware through other devices that the sensor is collecting information. The usability and efficacy of the notice are important considerations.

Related Controls: PT-1, PT-4, PT-5.

(5) SENSOR CAPABILITY AND DATA | COLLECTION MINIMIZATION

Employ [*Assignment: organization-defined sensors*] that are configured to minimize the collection of information about individuals that is not needed.

Discussion: Although policies to control for authorized use can be applied to information once it is collected, minimizing the collection of information that is not needed mitigates privacy risk at the system entry point and mitigates the risk of policy control failures. Sensor configurations include the obscuring of human features, such as blurring or pixelating flesh tones.

Related Controls: SA-8, SI-12.

References: [OMB A-130], [SP 800-124].

SC-43 USAGE RESTRICTIONS

Control:

a. Establish usage restrictions and implementation guidelines for the following system components: [*Assignment: organization-defined system components*]; and

b. Authorize, monitor, and control the use of such components within the system.

Discussion: Usage restrictions apply to all system components including but not limited to mobile code, mobile devices, wireless access, and wired and wireless peripheral components (e.g., copiers, printers, scanners, optical devices, and other similar technologies). The usage restrictions and implementation guidelines are based on the potential for system components to cause damage to the system and help to ensure that only authorized system use occurs.

Related Controls: AC-18, AC-19, CM-6, SC-7, SC-18.

Control Enhancements: None.

References: [OMB A-130], [SP 800-124].

SC-44 DETONATION CHAMBERS

Control: Employ a detonation chamber capability within [*Assignment: organization-defined system, system component, or location*].

Discussion: 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.

Control Enhancements: None.

References: [SP 800-177].

SC-45 SYSTEM TIME SYNCHRONIZATION

Control: Synchronize system clocks within and between systems and system components.

Discussion: 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.

Control Enhancements:

(1) SYSTEM TIME SYNCHRONIZATION | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

(a) Compare the internal system clocks [*Assignment: organization-defined frequency*] with [*Assignment: organization-defined authoritative time source*]; and

(b) Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [*Assignment: organization-defined time period*].

Discussion: 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.

(2) SYSTEM TIME SYNCHRONIZATION | SECONDARY AUTHORITATIVE TIME SOURCE

(a) Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source; and

(b) Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable.

Discussion: It may be necessary to employ geolocation information to determine that the secondary authoritative time source is in a different geographic region.

Related Controls: None.

References: [IETF 5905].

SC-46 CROSS DOMAIN POLICY ENFORCEMENT

Control: Implement a policy enforcement mechanism [*Selection: physically; logically*] between the physical and/or network interfaces for the connecting security domains.

Discussion: For logical policy enforcement mechanisms, organizations avoid creating a logical path between interfaces to prevent the ability to bypass the policy enforcement mechanism. For physical policy enforcement mechanisms, the robustness of physical isolation afforded by the physical implementation of policy enforcement to preclude the presence of logical covert channels penetrating the security domain may be needed. Contact ncdsmo@nsa.gov for more information.

Related Controls: AC-4, SC-7.

Control Enhancements: None.

References: [SP 800-160-1].

SC-47 ALTERNATE COMMUNICATIONS PATHS

Control: Establish [*Assignment: organization-defined alternate communications paths*] for system operations organizational command and control.

Discussion: An incident, whether adversarial- or nonadversarial-based, can disrupt established communications paths used for system operations and organizational command and control. Alternate communications paths reduce the risk of all communications paths being affected by the same incident. To compound the problem, the inability of organizational officials to obtain timely information about disruptions or to provide timely direction to operational elements after a communications path incident, can impact the ability of the organization to respond to such incidents in a timely manner. Establishing alternate communications paths for command and control purposes, including designating alternative decision makers if primary decision makers are unavailable and establishing the extent and limitations of their actions, can greatly facilitate the organization's ability to continue to operate and take appropriate actions during an incident.

Related Controls: CP-2, CP-8.

Control Enhancements: None.

References: [SP 800-34], [SP 800-61], [SP 800-160-2].

SC-48 SENSOR RELOCATION

Control: Relocate [*Assignment: organization-defined sensors and monitoring capabilities*] to [*Assignment: organization-defined locations*] under the following conditions or circumstances: [*Assignment: organization-defined conditions or circumstances*].

Discussion: Adversaries may take various paths and use different approaches as they move laterally through an organization (including its systems) to reach their target or as they attempt to exfiltrate information from the organization. The organization often only has a limited set of monitoring and detection capabilities, and they may be focused on the critical or likely infiltration or exfiltration paths. By using communications paths that the organization typically does not monitor, the adversary can increase its chances of achieving its desired goals. By relocating its sensors or monitoring capabilities to new locations, the organization can impede the adversary's ability to achieve its goals. The relocation of the sensors or monitoring capabilities might be done based on threat information that the organization has acquired or randomly to confuse the adversary and make its lateral transition through the system or organization more challenging.

Related Controls: AU-2, SC-7, SI-4.

Control Enhancements:

(1) SENSOR RELOCATION | DYNAMIC RELOCATION OF SENSORS OR MONITORING CAPABILITIES

Dynamically relocate [*Assignment: organization-defined sensors and monitoring capabilities*] to [*Assignment: organization-defined locations*] under the following conditions or circumstances: [*Assignment: organization-defined conditions or circumstances*].

Discussion: None.

Related Controls: None.

References: [SP 800-160-2].

SC-49 HARDWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT

Control: Implement hardware-enforced separation and policy enforcement mechanisms between [*Assignment: organization-defined security domains*].

Discussion: System owners may require additional strength of mechanism and robustness to ensure domain separation and policy enforcement for specific types of threats and environments of operation. Hardware-enforced separation and policy enforcement provide greater strength of mechanism than software-enforced separation and policy enforcement.

Related Controls: AC-4, SA-8, SC-50.

Control Enhancements: None.

References: [SP 800-160-1].

SC-50 SOFTWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT

Control: Implement software-enforced separation and policy enforcement mechanisms between [*Assignment: organization-defined security domains*].

Discussion: System owners may require additional strength of mechanism to ensure domain separation and policy enforcement for specific types of threats and environments of operation.

Related Controls: AC-3, AC-4, SA-8, SC-2, SC-3, SC-49.

Control Enhancements: None.

References: [SP 800-160-1].

SC-51 HARDWARE-BASED PROTECTION

Control:

a. Employ hardware-based, write-protect for [*Assignment: organization-defined system firmware components*]; and

b. Implement specific procedures for [*Assignment: organization-defined authorized individuals*] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.

Discussion: None.

Related Controls: None.

Control Enhancements: None.

References: None.