3.19 SYSTEM AND INFORMATION INTEGRITY

Quick link to System and Information Integrity Summary Table

SI-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 information integrity 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 information integrity policy and the associated system and information integrity controls;

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

c. Review and update the current system and information integrity:

   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 information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and information integrity policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

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

Control Enhancements: None.

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

SI-2 FLAW REMEDIATION

Control:

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

Discussion: The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified.

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

Related Controls: CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI-5, SI-7, SI-11.

Control Enhancements:

(1) FLAW REMEDIATION | CENTRAL MANAGEMENT

[Withdrawn: Incorporated into PL-9.]

(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

Determine if system components have applicable security-relevant software and firmware updates installed using [*Assignment: organization-defined automated mechanisms*] [*Assignment: organization-defined frequency*].

Discussion: Automated mechanisms can track and determine the status of known flaws for system components.

Related Controls: CA-7, SI-4.

(3) FLAW REMEDIATION | TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS

(a) Measure the time between flaw identification and flaw remediation; and

(b) Establish the following benchmarks for taking corrective actions: [*Assignment: organization-defined benchmarks*].

Discussion: Organizations determine the time it takes on average to correct system flaws after such flaws have been identified and subsequently establish organizational benchmarks

(i.e., time frames) for taking corrective actions. Benchmarks can be established by the type of flaw or the severity of the potential vulnerability if the flaw can be exploited.

Related Controls: None.

(4) FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS

Employ automated patch management tools to facilitate flaw remediation to the following system components: [*Assignment: organization-defined system components*].

Discussion: Using automated tools to support patch management helps to ensure the timeliness and completeness of system patching operations.

Related Controls: None.

(5) FLAW REMEDIATION | AUTOMATIC SOFTWARE AND FIRMWARE UPDATES

Install [*Assignment: organization-defined security-relevant software and firmware updates*] automatically to [*Assignment: organization-defined system components*].

Discussion: Due to system integrity and availability concerns, organizations consider the methodology used to carry out automatic updates. Organizations balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and control with any mission or operational impacts that automatic updates might impose.

Related Controls: None.

(6) FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE AND FIRMWARE

Remove previous versions of [*Assignment: organization-defined software and firmware components*] after updated versions have been installed.

Discussion: Previous versions of software or firmware components that are not removed from the system after updates have been installed may be exploited by adversaries. Some products may automatically remove previous versions of software and firmware from the system.

Related Controls: None.

References: [OMB A-130], [FIPS 140-3], [FIPS 186-4], [SP 800-39], [SP 800-40], [SP 800-128], [IR 7788].

SI-3 MALICIOUS CODE PROTECTION

Control:

a. Implement [*Selection (one or more): signature based; non-signature based*] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at [*Selection (one or more): endpoint; network entry and exit points*] as the files are downloaded, opened, or executed in accordance with organizational policy; and

2. [*Selection (one or more): block malicious code; quarantine malicious code; take* [*Assignment: organization-defined action*]]; and send alert to [*Assignment: organization-defined personnel or roles*] in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Discussion: System entry and exit points include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the world-wide web, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code.

Malicious code protection mechanisms include both signature- and nonsignature-based technologies. Nonsignature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Nonsignature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software as well as custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.

In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended. Organizations may determine that, in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, the detection of malicious downloads, or the detection of maliciousness when attempting to open or execute files.

Related Controls: AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, PL-9, RA-5, SC-7, SC-23, SC-26, SC-28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15.

Control Enhancements:

(1) MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT

[Withdrawn: Incorporated into PL-9.]

(2) MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES

[Withdrawn: Incorporated into SI-3.]

(3) MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS

[Withdrawn: Incorporated into AC-6(10).]

(4) MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED USERS

Update malicious code protection mechanisms only when directed by a privileged user.

Discussion: Protection mechanisms for malicious code are typically categorized as security-related software and, as such, are only updated by organizational personnel with appropriate access privileges.

Related Controls: CM-5.

(5) MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES

[Withdrawn: Incorporated into MP-7.]

(6) MALICIOUS CODE PROTECTION | TESTING AND VERIFICATION

(a) Test malicious code protection mechanisms [*Assignment: organization-defined frequency*] by introducing known benign code into the system; and

(b) Verify that the detection of the code and the associated incident reporting occur.

Discussion: None.

Related Controls: CA-2, CA-7, RA-5.

(7) MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION

[Withdrawn: Incorporated into SI-3.]

(8) MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS

(a) Detect the following unauthorized operating system commands through the kernel application programming interface on [*Assignment: organization-defined system hardware components*]: [*Assignment: organization-defined unauthorized operating system commands*]; and

(b) [*Selection (one or more): issue a warning; audit the command execution; prevent the execution of the command*].

Discussion: Detecting unauthorized commands can be applied to critical interfaces other than kernel-based interfaces, including interfaces with virtual machines and privileged applications. Unauthorized operating system commands include commands for kernel functions from system processes that are not trusted to initiate such commands as well as commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate. Organizations can define the malicious commands to be detected by a combination of command types, command classes, or specific instances of commands. Organizations can also define hardware components by component type, component, component location in the network, or a combination thereof. Organizations may select different actions for different types, classes, or instances of malicious commands.

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

(9) MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS

[Withdrawn: Moved to AC-17(10).]

(10) MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS

(a) Employ the following tools and techniques to analyze the characteristics and behavior of malicious code: [*Assignment: organization-defined tools and techniques*]; and

(b) Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.

Discussion: The use of malicious code analysis tools provides organizations with a more in-depth understanding of adversary tradecraft (i.e., tactics, techniques, and procedures) and the functionality and purpose of specific instances of malicious code. Understanding the characteristics of malicious code facilitates effective organizational responses to current and future threats. Organizations can conduct malicious code analyses by employing reverse engineering techniques or by monitoring the behavior of executing code.

Related Controls: None.

References: [SP 800-83], [SP 800-125B], [SP 800-177].

SI-4 SYSTEM MONITORING

Control:

a. Monitor the system to detect:

   1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [*Assignment: organization-defined monitoring objectives*]; and

   2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: [*Assignment: organization-defined techniques and methods*];

c. Invoke internal monitoring capabilities or deploy monitoring devices:

   1. Strategically within the system to collect organization-determined essential information; and

   2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide [*Assignment: organization-defined system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed;* [*Assignment: organization-defined frequency*]].

Discussion: System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other controls (e.g., AC-2g, AC-2(7), AC-2(12)(a), AC-17(1), AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, MA-3a, MA-4a, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b). Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10.

Control Enhancements:

(1) SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

Discussion: Linking individual intrusion detection tools into a system-wide intrusion detection system provides additional coverage and effective detection capabilities. The information contained in one intrusion detection tool can be shared widely across the organization, making the system-wide detection capability more robust and powerful.

Related Controls: None.

(2) SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS

Employ automated tools and mechanisms to support near real-time analysis of events.

Discussion: Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls: PM-23, PM-25.

(3) SYSTEM MONITORING | AUTOMATED TOOL AND MECHANISM INTEGRATION

Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms.

Discussion: Using automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access and flow control mechanisms facilitates a rapid response to attacks by enabling the reconfiguration of mechanisms in support of attack isolation and elimination.

Related Controls: PM-23, PM-25.

(4) SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;

(b) Monitor inbound and outbound communications traffic [*Assignment: organization-defined frequency*] for [*Assignment: organization-defined unusual or unauthorized activities or conditions*].

Discussion: Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

Related Controls: None.

(5) SYSTEM MONITORING | SYSTEM-GENERATED ALERTS

Alert [*Assignment: organization-defined personnel or roles*] when the following system-generated indications of compromise or potential compromise occur: [*Assignment: organization-defined compromise indicators*].

Discussion: Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations in SI-4(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

Related Controls: AU-4, AU-5, PE-6.

(6) SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS

[Withdrawn: Incorporated into AC-6(10).]

(7) SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS

(a) Notify [*Assignment: organization-defined incident response personnel (identified by name and/or by role)*] of detected suspicious events; and

(b) Take the following actions upon detection: [*Assignment: organization-defined least-disruptive actions to terminate suspicious events*].

Discussion: Least-disruptive actions include initiating requests for human responses.

Related Controls: None.

(8) SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION

[Withdrawn: Incorporated into SI-4.]

(9) SYSTEM MONITORING | TESTING OF MONITORING TOOLS AND MECHANISMS

Test intrusion-monitoring tools and mechanisms [*Assignment: organization-defined frequency*].

Discussion: Testing intrusion-monitoring tools and mechanisms is necessary to ensure that the tools and mechanisms are operating correctly and continue to satisfy the monitoring objectives of organizations. The frequency and depth of testing depends on the types of tools and mechanisms used by organizations and the methods of deployment.

Related Controls: None.

(10) SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS

Make provisions so that [*Assignment: organization-defined encrypted communications traffic*] is visible to [*Assignment: organization-defined system monitoring tools and mechanisms*].

Discussion: Organizations balance the need to encrypt communications traffic to protect data confidentiality with the need to maintain visibility into such traffic from a monitoring perspective. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.

Related Controls: None.

(11) SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES

Analyze outbound communications traffic at the external interfaces to the system and selected [*Assignment: organization-defined interior points within the system*] to discover anomalies.

Discussion: Organization-defined interior points include subnetworks and subsystems. Anomalies within organizational systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols (e.g., IPv6 usage during IPv4 transition), and attempted communications with suspected malicious external addresses.

Related Controls: None.

(12) SYSTEM MONITORING | AUTOMATED ORGANIZATION-GENERATED ALERTS

Alert [*Assignment: organization-defined personnel or roles*] using [*Assignment: organization-defined automated mechanisms*] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [*Assignment: organization-defined activities that trigger alerts*].

Discussion: Organizational personnel on the system alert notification list include system administrators, mission or business owners, system owners, senior agency information security officer, senior agency official for privacy, system security officers, or privacy officers. Automated organization-generated alerts are the security alerts generated by organizations and transmitted using automated means. The sources for organization-generated alerts are focused on other entities such as suspicious activity reports and reports on potential insider threats. In contrast to alerts generated by the organization, alerts generated by the system in SI-4(5) focus on information sources that are internal to the systems, such as audit records.

Related Controls: None.

(13) SYSTEM MONITORING | ANALYZE TRAFFIC AND EVENT PATTERNS

(a) Analyze communications traffic and event patterns for the system;

(b) Develop profiles representing common traffic and event patterns; and

(c) Use the traffic and event profiles in tuning system-monitoring devices.

Discussion: Identifying and understanding common communications traffic and event patterns help organizations provide useful information to system monitoring devices to more effectively identify suspicious or anomalous traffic and events when they occur. Such information can help reduce the number of false positives and false negatives during system monitoring.

Related Controls: None.

(14) SYSTEM MONITORING | WIRELESS INTRUSION DETECTION

Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

Discussion: Wireless signals may radiate beyond organizational facilities. Organizations proactively search for unauthorized wireless connections, including the conduct of thorough scans for unauthorized wireless access points. Wireless scans are not limited to those areas within facilities containing systems but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational systems.

Related Controls: AC-18, IA-3.

(15) SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS

Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

Discussion: Wireless networks are inherently less secure than wired networks. For example, wireless networks are more susceptible to eavesdroppers or traffic analysis than wireline networks. When wireless to wireline communications exist, the wireless network could become a port of entry into the wired network. Given the greater facility of unauthorized network access via wireless access points compared to unauthorized wired network access from within the physical boundaries of the system, additional monitoring of transitioning traffic between wireless and wired networks may be necessary to detect malicious activities. Employing intrusion detection systems to monitor wireless communications traffic helps to ensure that the traffic does not contain malicious code prior to transitioning to the wireline network.

Related Controls: AC-18.

(16) SYSTEM MONITORING | CORRELATE MONITORING INFORMATION

Correlate information from monitoring tools and mechanisms employed throughout the system.

Discussion: Correlating information from different system monitoring tools and mechanisms can provide a more comprehensive view of system activity. Correlating system monitoring tools and mechanisms that typically work in isolation—including malicious code protection software, host monitoring, and network monitoring—can provide an organization-wide monitoring view and may reveal otherwise unseen attack patterns. Understanding the capabilities and limitations of diverse monitoring tools and mechanisms and how to maximize the use of information generated by those tools and mechanisms can help organizations develop, operate, and maintain effective monitoring programs. The correlation of monitoring information is especially important during the transition from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

Related Controls: AU-6.

(17) SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS

Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.

Discussion: Correlating monitoring information from a more diverse set of information sources helps to achieve integrated situational awareness. Integrated situational awareness from a combination of physical, cyber, and supply chain monitoring activities enhances the capability of organizations to more quickly detect sophisticated attacks and investigate the methods and techniques employed to carry out such attacks. In contrast to SI-4(16), which correlates the various cyber monitoring information, integrated situational awareness is intended to correlate monitoring beyond the cyber domain. Correlation of monitoring information from multiple activities may help reveal attacks on organizations that are operating across multiple attack vectors.

Related Controls: AU-16, PE-6, SR-2, SR-4, SR-6.

(18) SYSTEM MONITORING | ANALYZE TRAFFIC AND COVERT EXFILTRATION

Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [*Assignment: organization-defined interior points within the system*].

Discussion: Organization-defined interior points include subnetworks and subsystems. Covert means that can be used to exfiltrate information include steganography.

Related Controls: None.

(19) SYSTEM MONITORING | RISK FOR INDIVIDUALS

Implement [*Assignment: organization-defined additional monitoring*] of individuals who have been identified by [*Assignment: organization-defined sources*] as posing an increased level of risk.

Discussion: Indications of increased risk from individuals can be obtained from different sources, including personnel records, intelligence agencies, law enforcement organizations, and other sources. The monitoring of individuals is coordinated with the management, legal, security, privacy, and human resource officials who conduct such monitoring. Monitoring is conducted in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: None.

(20) SYSTEM MONITORING | PRIVILEGED USERS

Implement the following additional monitoring of privileged users: [*Assignment: organization-defined additional monitoring*].

Discussion: Privileged users have access to more sensitive information, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to systems and organizations than non-privileged users. Therefore, implementing additional monitoring on privileged users helps to ensure that organizations can identify malicious activity at the earliest possible time and take appropriate actions.

Related Controls: AC-18.

(21) SYSTEM MONITORING | PROBATIONARY PERIODS

Implement the following additional monitoring of individuals during [*Assignment: organization-defined probationary period*]: [*Assignment: organization-defined additional monitoring*].

Discussion: During probationary periods, employees do not have permanent employment status within organizations. Without such status or access to information that is resident on the system, additional monitoring can help identify any potentially malicious activity or inappropriate behavior.

Related Controls: AC-18.

(22) SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES

(a) Detect network services that have not been authorized or approved by [*Assignment: organization-defined authorization or approval processes*]; and

(b) [*Selection (one or more): Audit; Alert* [*Assignment: organization-defined personnel or roles*]] when detected.

Discussion: Unauthorized or unapproved network services include services in service-oriented architectures that lack organizational verification or validation and may therefore be unreliable or serve as malicious rogues for valid services.

Related Controls: CM-7.

(23) SYSTEM MONITORING | HOST-BASED DEVICES

Implement the following host-based monitoring mechanisms at [*Assignment: organization-defined system components*]: [*Assignment: organization-defined host-based monitoring mechanisms*].

Discussion: Host-based monitoring collects information about the host (or system in which it resides). System components in which host-based monitoring can be implemented include servers, notebook computers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple product developers or vendors.

Related Controls: AC-18, AC-19.

(24) SYSTEM MONITORING | INDICATORS OF COMPROMISE

Discover, collect, and distribute to [*Assignment: organization-defined personnel or roles*], indicators of compromise provided by [*Assignment: organization-defined sources*].

Discussion: Indicators of compromise (IOC) are forensic artifacts from intrusions that are identified on organizational systems at the host or network level. IOCs provide valuable information on systems that have been compromised. IOCs can include the creation of registry key values. IOCs for network traffic include Universal Resource Locator or protocol elements that indicate malicious code command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that systems and organizations are vulnerable to the same exploit or attack. Threat indicators, signatures, tactics, techniques, procedures, and other indicators of compromise may be available via government and non-government cooperatives, including the Forum of Incident Response and Security Teams, the United States Computer Emergency Readiness Team, the Defense Industrial Base Cybersecurity Information Sharing Program, and the CERT Coordination Center.

Related Controls: AC-18.

(25) SYSTEM MONITORING | OPTIMIZE NETWORK TRAFFIC ANALYSIS

Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.

Discussion: Encrypted traffic, asymmetric routing architectures, capacity and latency limitations, and transitioning from older to newer technologies (e.g., IPv4 to IPv6 network protocol transition) may result in blind spots for organizations when analyzing network traffic. Collecting, decrypting, pre-processing, and distributing only relevant traffic to monitoring devices can streamline the efficiency and use of devices and optimize traffic analysis.

Related Controls: None.

References: [OMB A-130], [FIPS 140-3], [SP 800-61], [SP 800-83], [SP 800-92], [SP 800-94], [SP 800-137].

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control:

a. Receive system security alerts, advisories, and directives from [*Assignment: organization-defined external organizations*] on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to: [*Selection (one or more):* [*Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined elements within the organization*]; [*Assignment: organization-defined external organizations*]]; and

d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

Discussion: The Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness throughout the Federal Government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include supply chain

partners, external mission or business partners, external service providers, and other peer or supporting organizations.

Related Controls: PM-15, RA-5, SI-2.

Control Enhancements:

(1) SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES

Broadcast security alert and advisory information throughout the organization using [*Assignment: organization-defined automated mechanisms*].

Discussion: The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational mission and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three levels related to the management of risk, including the governance level, mission and business process level, and the information system level.

Related Controls: None.

References: [SP 800-40].

SI-6 SECURITY AND PRIVACY FUNCTION VERIFICATION

Control:

a. Verify the correct operation of [*Assignment: organization-defined security and privacy functions*];

b. Perform the verification of the functions specified in SI-6a [*Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency*]];

c. Alert [*Assignment: organization-defined personnel or roles*] to failed security and privacy verification tests; and

d. [*Selection (one or more): Shut the system down; Restart the system; [Assignment: organization-defined alternative action(s)*]] when anomalies are discovered.

Discussion: Transitional states for systems include system startup, restart, shutdown, and abort. System notifications include hardware indicator lights, electronic alerts to system administrators, and messages to local computer consoles. In contrast to security function verification, privacy function verification ensures that privacy functions operate as expected and are approved by the senior agency official for privacy or that privacy attributes are applied or used as expected.

Related Controls: CA-7, CM-4, CM-6, SI-7.

Control Enhancements:

(1) SECURITY AND PRIVACY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS

[Withdrawn: Incorporated into SI-6.]

(2) SECURITY AND PRIVACY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING

Implement automated mechanisms to support the management of distributed security and privacy function testing.

Discussion: The use of automated mechanisms to support the management of distributed function testing helps to ensure the integrity, timeliness, completeness, and efficacy of such testing.

Related Controls: SI-2.

(3) SECURITY AND PRIVACY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS

Report the results of security and privacy function verification to [*Assignment: organization-defined personnel or roles*].

Discussion: Organizational personnel with potential interest in the results of the verification of security and privacy functions include systems security officers, senior agency information security officers, and senior agency officials for privacy.

Related Controls: SI-4, SR-4, SR-5.

References: [OMB A-130].

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Control:

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [*Assignment: organization-defined software, firmware, and information*]; and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [*Assignment: organization-defined actions*].

Discussion: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

Related Controls: AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11.

Control Enhancements:

(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS

Perform an integrity check of [*Assignment: organization-defined software, firmware, and information*] [*Selection (one or more):* at startup; at [*Assignment: organization-defined transitional states or security-relevant events*]; [*Assignment: organization-defined frequency*]].

Discussion: Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort.

Related Controls: None.

(2) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS

Employ automated tools that provide notification to [*Assignment: organization-defined personnel or roles*] upon discovering discrepancies during integrity verification.

Discussion: The employment of automated tools to report system and information integrity violations and to notify organizational personnel in a timely matter is essential to effective risk response. Personnel with an interest in system and information integrity violations include mission and business owners, system owners, senior agency information security official, senior agency official for privacy, system administrators, software developers, systems integrators, information security officers, and privacy officers.

Related Controls: None.

(3) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY MANAGED INTEGRITY TOOLS

Employ centrally managed integrity verification tools.

Discussion: Centrally managed integrity verification tools provides greater consistency in the application of such tools and can facilitate more comprehensive coverage of integrity verification actions.

Related Controls: AU-3, SI-2, SI-8.

(4) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER-EVIDENT PACKAGING

[Withdrawn: Incorporated into SR-9.]

(5) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS

Automatically [*Selection (one or more): shut the system down; restart the system; implement* [*Assignment: organization-defined controls*]] when integrity violations are discovered.

Discussion: Organizations may define different integrity-checking responses by type of information, specific information, or a combination of both. Types of information include firmware, software, and user data. Specific information includes boot firmware for certain types of machines. The automatic implementation of controls within organizational systems includes reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur.

Related Controls: None.

(6) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

Discussion: Cryptographic mechanisms used to protect integrity include digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Organizations that employ cryptographic mechanisms also consider cryptographic key management solutions.

Related Controls: SC-12, SC-13.

(7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [*Assignment: organization-defined security-relevant changes to the system*].

Discussion: Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include

unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

Related Controls: AU-2, AU-6, IR-4, IR-5, SI-4.

(8) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS

Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: [*Selection (one or more): generate an audit record; alert current user; alert* [*Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined other actions*]].

Discussion: Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations.

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

(9) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS

Verify the integrity of the boot process of the following system components: [*Assignment: organization-defined system components*].

Discussion: Ensuring the integrity of boot processes is critical to starting system components in known, trustworthy states. Integrity verification mechanisms provide a level of assurance that only trusted code is executed during boot processes.

Related Controls: SI-6.

(10) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE

Implement the following mechanisms to protect the integrity of boot firmware in [*Assignment: organization-defined system components*]: [*Assignment: organization-defined mechanisms*].

Discussion: Unauthorized modifications to boot firmware may indicate a sophisticated, targeted attack. These types of targeted attacks can result in a permanent denial of service or a persistent malicious code presence. These situations can occur if the firmware is corrupted or if the malicious code is embedded within the firmware. System components can protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of all updates to the firmware prior to applying changes to the system component and preventing unauthorized processes from modifying the boot firmware.

Related Controls: SI-6.

(11) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES

[Withdrawn: Moved to CM-7(6).]

(12) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION

Require that the integrity of the following user-installed software be verified prior to execution: [*Assignment: organization-defined user-installed software*].

Discussion: Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or programs that contains errors from unauthorized modifications. Organizations consider the practicality of approaches to verifying software integrity, including the availability of trustworthy checksums from software developers and vendors.

Related Controls: CM-11.

(13) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS

[Withdrawn: Moved to CM-7(7).]

(14) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE

[Withdrawn: Moved to CM-7(8).]

(15) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION

Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [*Assignment: organization-defined software or firmware components*].

Discussion: Cryptographic authentication includes verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code. Organizations that employ cryptographic mechanisms also consider cryptographic key management solutions.

Related Controls: CM-5, SC-12, SC-13.

(16) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION

Prohibit processes from executing without supervision for more than [*Assignment: organization-defined time period*].

Discussion: Placing a time limit on process execution without supervision is intended to apply to processes for which typical or normal execution periods can be determined and situations in which organizations exceed such periods. Supervision includes timers on operating systems, automated responses, and manual oversight and response when system process anomalies occur.

Related Controls: None.

(17) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | RUNTIME APPLICATION SELF-PROTECTION

Implement [*Assignment: organization-defined controls*] for application self-protection at runtime.

Discussion: Runtime application self-protection employs runtime instrumentation to detect and block the exploitation of software vulnerabilities by taking advantage of information from the software in execution. Runtime exploit prevention differs from traditional perimeter-based protections such as guards and firewalls which can only detect and block attacks by using network information without contextual awareness. Runtime application self-protection technology can reduce the susceptibility of software to attacks by monitoring its inputs and blocking those inputs that could allow attacks. It can also help protect the runtime environment from unwanted changes and tampering. When a threat is detected, runtime application self-protection technology can prevent exploitation and take other actions (e.g., sending a warning message to the user, terminating the user's session, terminating the application, or sending an alert to organizational personnel). Runtime application self-protection solutions can be deployed in either a monitor or protection mode.

Related Controls: SI-16.

References: [OMB A-130], [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-70], [SP 800-147].

SI-8 SPAM PROTECTION

Control:

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Discussion: System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions.

Related Controls: PL-9, SC-5, SC-7, SC-38, SI-3, SI-4.

Control Enhancements:

(1) SPAM PROTECTION | CENTRAL MANAGEMENT

[Withdrawn: Incorporated into PL-9.]

(2) SPAM PROTECTION | AUTOMATIC UPDATES

Automatically update spam protection mechanisms [*Assignment: organization-defined frequency*].

Discussion: Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capabilities.

Related Controls: None.

(3) SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY

Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.

Discussion: Learning mechanisms include Bayesian filters that respond to user inputs that identify specific traffic as spam or legitimate by updating algorithm parameters and thereby more accurately separating types of traffic.

Related Controls: None.

References: [SP 800-45], [SP 800-177].

SI-9 INFORMATION INPUT RESTRICTIONS

[Withdrawn: Incorporated into AC-2, AC-3, AC-5, and AC-6.]

SI-10 INFORMATION INPUT VALIDATION

Control: Check the validity of the following information inputs: [*Assignment: organization-defined information inputs to the system*].

Discussion: Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of "387," "abc," or "%K%" are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data

to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

Related Controls: None.

Control Enhancements:

(1) INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY

(a) Provide a manual override capability for input validation of the following information inputs: [*Assignment: organization-defined inputs defined in the base control (SI-10)*];

(b) Restrict the use of the manual override capability to only [*Assignment: organization-defined authorized individuals*]; and

(c) Audit the use of the manual override capability.

Discussion: In certain situations, such as during events that are defined in contingency plans, a manual override capability for input validation may be needed. Manual overrides are used only in limited circumstances and with the inputs defined by the organization.

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

(2) INFORMATION INPUT VALIDATION | REVIEW AND RESOLVE ERRORS

Review and resolve input validation errors within [*Assignment: organization-defined time period*].

Discussion: Resolution of input validation errors includes correcting systemic causes of errors and resubmitting transactions with corrected input. Input validation errors are those related to the information inputs defined by the organization in the base control (SI-10).

Related Controls: None.

(3) INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR

Verify that the system behaves in a predictable and documented manner when invalid inputs are received.

Discussion: A common vulnerability in organizational systems is unpredictable behavior when invalid inputs are received. Verification of system predictability helps ensure that the system behaves as expected when invalid inputs are received. This occurs by specifying system responses that allow the system to transition to known states without adverse, unintended side effects. The invalid inputs are those related to the information inputs defined by the organization in the base control (SI-10).

Related Controls: None.

(4) INFORMATION INPUT VALIDATION | TIMING INTERACTIONS

Account for timing interactions among system components in determining appropriate responses for invalid inputs.

Discussion: In addressing invalid system inputs received across protocol interfaces, timing interactions become relevant, where one protocol needs to consider the impact of the error response on other protocols in the protocol stack. For example, 802.11 standard wireless network protocols do not interact well with Transmission Control Protocols (TCP) when packets are dropped (which could be due to invalid packet input). TCP assumes packet losses are due to congestion, while packets lost over 802.11 links are typically dropped due to noise or collisions on the link. If TCP makes a congestion response, it takes the wrong action in response to a collision event. Adversaries may be able to use what appear to be acceptable individual behaviors of the protocols in concert to achieve adverse effects through suitable

construction of invalid input. The invalid inputs are those related to the information inputs defined by the organization in the base control (SI-10).

Related Controls: None.

(5) INFORMATION INPUT VALIDATION | RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS

Restrict the use of information inputs to [*Assignment: organization-defined trusted sources*] and/or [*Assignment: organization-defined formats*].

Discussion: Restricting the use of inputs to trusted sources and in trusted formats applies the concept of authorized or permitted software to information inputs. Specifying known trusted sources for information inputs and acceptable formats for such inputs can reduce the probability of malicious activity. The information inputs are those defined by the organization in the base control (SI-10).

Related Controls: AC-3, AC-6.

(6) INFORMATION INPUT VALIDATION | INJECTION PREVENTION

Prevent untrusted data injections.

Discussion: Untrusted data injections may be prevented using a parameterized interface or output escaping (output encoding). Parameterized interfaces separate data from code so that injections of malicious or unintended data cannot change the semantics of commands being sent. Output escaping uses specified characters to inform the interpreter's parser whether data is trusted. Prevention of untrusted data injections are with respect to the information inputs defined by the organization in the base control (SI-10).

Related Controls: AC-3, AC-6.

References: [OMB A-130].

SI-11 ERROR HANDLING

Control:

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to [*Assignment: organization-defined personnel or roles*].

Discussion: Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

Related Controls: AU-2, AU-3, SC-31, SI-2, SI-15.

Control Enhancements: None.

References: None.

SI-12 INFORMATION MANAGEMENT AND RETENTION

Control: Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

Discussion: Information management and retention requirements cover the full life cycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative information. The National Archives and Records Administration (NARA) provides federal policy and guidance on records retention and schedules. If organizations have a records management office, consider coordinating with records management personnel. Records produced from the output of implemented controls that may require management and retention include, but are not limited to: All XX-1, AC-6(9), AT-4, AU-12, CA-2, CA-3, CA-5, CA-6, CA-7, CA-8, CA-9, CM-2, CM-3, CM-4, CM-6, CM-8, CM-9, CM-12, CM-13, CP-2, IR-6, IR-8, MA-2, MA-4, PE-2, PE-8, PE-16, PE-17, PL-2, PL-4, PL-7, PL-8, PM-5, PM-8, PM-9, PM-18, PM-21, PM-27, PM-28, PM-30, PM-31, PS-2, PS-6, PS-7, PT-2, PT-3, PT-7, RA-2, RA-3, RA-5, RA-8, SA-4, SA-5, SA-8, SA-10, SI-4, SR-2, SR-4, SR-8.

Related Controls: All XX-1 Controls, AC-16, AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM-5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PL-2, PL-4, PM-4, PM-8, PM-9, PS-2, PS-6, PT-2, PT-3, RA-2, RA-3, SA-5, SA-8, SR-2.

Control Enhancements:

(1) INFORMATION MANAGEMENT AND RETENTION | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [*Assignment: organization-defined elements of personally identifiable information*].

Discussion: Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for operational purposes helps to reduce the level of privacy risk created by a system. The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining which elements of personally identifiable information may create risk.

Related Controls: PM-25.

(2) INFORMATION MANAGEMENT AND RETENTION | MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH

Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [*Assignment: organization-defined techniques*].

Discussion: Organizations can minimize the risk to an individual's privacy by employing techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining the techniques to use and when to use them.

Related Controls: PM-22, PM-25, SI-19.

(3) INFORMATION MANAGEMENT AND RETENTION | INFORMATION DISPOSAL

Use the following techniques to dispose of, destroy, or erase information following the retention period: [*Assignment: organization-defined techniques*].

Discussion: Organizations can minimize both security and privacy risks by disposing of information when it is no longer needed. The disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.

Related Controls: None.

References: [USC 2901], [OMB A-130].

SI-13 PREDICTABLE FAILURE PREVENTION

Control:

a. Determine mean time to failure (MTTF) for the following system components in specific environments of operation: [*Assignment: organization-defined system components*]; and

b. Provide substitute system components and a means to exchange active and standby components in accordance with the following criteria: [*Assignment: organization-defined MTTF substitution criteria*].

Discussion: While MTTF is primarily a reliability issue, predictable failure prevention is intended to address potential failures of system components that provide security capabilities. Failure rates reflect installation-specific consideration rather than the industry-average. Organizations define the criteria for the substitution of system components based on the MTTF value with consideration for the potential harm from component failures. The transfer of responsibilities between active and standby components does not compromise safety, operational readiness, or security capabilities. The preservation of system state variables is also critical to help ensure a successful transfer process. Standby components remain available at all times except for maintenance issues or recovery failures in progress.

Related Controls: CP-2, CP-10, CP-13, MA-2, MA-6, SA-8, SC-6.

Control Enhancements:

(1) PREDICTABLE FAILURE PREVENTION | TRANSFERRING COMPONENT RESPONSIBILITIES

Take system components out of service by transferring component responsibilities to substitute components no later than [*Assignment: organization-defined fraction or percentage*] of mean time to failure.

Discussion: Transferring primary system component responsibilities to other substitute components prior to primary component failure is important to reduce the risk of degraded or debilitated mission or business functions. Making such transfers based on a percentage of mean time to failure allows organizations to be proactive based on their risk tolerance. However, the premature replacement of system components can result in the increased cost of system operations.

Related Controls: None.

(2) PREDICTABLE FAILURE PREVENTION | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION

[Withdrawn: Incorporated into SI-7(16).]

(3) PREDICTABLE FAILURE PREVENTION | MANUAL TRANSFER BETWEEN COMPONENTS

Manually initiate transfers between active and standby system components when the use of the active component reaches [*Assignment: organization-defined percentage*] of the mean time to failure.

Discussion: For example, if the MTTF for a system component is 100 days and the MTTF percentage defined by the organization is 90 percent, the manual transfer would occur after 90 days.

Related Controls: None.

(4) PREDICTABLE FAILURE PREVENTION | STANDBY COMPONENT INSTALLATION AND NOTIFICATION

If system component failures are detected:

(a) Ensure that the standby components are successfully and transparently installed within [*Assignment: organization-defined time period*]; and

(b) [*Selection (one or more): Activate* [*Assignment: organization-defined alarm*]; *Automatically shut down the system;* [*Assignment: organization-defined action*]].

Discussion: Automatic or manual transfer of components from standby to active mode can occur upon the detection of component failures.

Related Controls: None.

(5) PREDICTABLE FAILURE PREVENTION | FAILOVER CAPABILITY

Provide [*Selection: real-time; near real-time*] [*Assignment: organization-defined failover capability*] *for the system*.

Discussion: Failover refers to the automatic switchover to an alternate system upon the failure of the primary system. Failover capability includes incorporating mirrored system operations at alternate processing sites or periodic data mirroring at regular intervals defined by the recovery time periods of organizations.

Related Controls: CP-6, CP-7, CP-9.

References: None.

SI-14 NON-PERSISTENCE

Control: Implement non-persistent [*Assignment: organization-defined system components and services*] that are initiated in a known state and terminated [*Selection (one or more): upon end of session of use; periodically at* [*Assignment: organization-defined frequency*]].

Discussion: Implementation of non-persistent components and services mitigates risk from advanced persistent threats (APTs) by reducing the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete attacks. By implementing the concept of non-persistence for selected system components, organizations can provide a trusted, known state computing resource for a specific time period that does not give adversaries sufficient time to exploit vulnerabilities in organizational systems or operating environments. Since the APT is a high-end, sophisticated threat with regard to capability, intent, and targeting, organizations assume that over an extended period, a percentage of attacks will be successful. Non-persistent system components and services are activated as required using protected information and terminated periodically or at the end of sessions. Non-persistence increases the work factor of adversaries attempting to compromise or breach organizational systems.

Non-persistence can be achieved by refreshing system components, periodically reimaging components, or using a variety of common virtualization techniques. Non-persistent services can be implemented by using virtualization techniques as part of virtual machines or as new instances of processes on physical machines (either persistent or non-persistent). The benefit of periodic refreshes of system components and services is that it does not require organizations to first determine whether compromises of components or services have occurred (something that may often be difficult to determine). The refresh of selected system components and services occurs with sufficient frequency to prevent the spread or intended impact of attacks, but not with such frequency that it makes the system unstable. Refreshes of critical components and services may be done periodically to hinder the ability of adversaries to exploit optimum windows of vulnerabilities.

Related Controls: SC-30, SC-34, SI-21.

Control Enhancements:

(1) NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES

Obtain software and data employed during system component and service refreshes from the following trusted sources: [*Assignment: organization-defined trusted sources*].

Discussion: Trusted sources include software and data from write-once, read-only media or from selected offline secure storage facilities.

Related Controls: None.

(2) NON-PERSISTENCE | NON-PERSISTENT INFORMATION

(a) [*Selection: Refresh* [*Assignment: organization-defined information*] [*Assignment: organization-defined frequency*]; *Generate* [*Assignment: organization-defined information*] *on demand*]; and

(b) Delete information when no longer needed.

Discussion: Retaining information longer than is needed makes the information a potential target for advanced adversaries searching for high value assets to compromise through unauthorized disclosure, unauthorized modification, or exfiltration. For system-related information, unnecessary retention provides advanced adversaries information that can assist in their reconnaissance and lateral movement through the system.

Related Controls: None.

(3) NON-PERSISTENCE | NON-PERSISTENT CONNECTIVITY

Establish connections to the system on demand and terminate connections after [*Selection: completion of a request; a period of non-use*].

Discussion: Persistent connections to systems can provide advanced adversaries with paths to move laterally through systems and potentially position themselves closer to high value assets. Limiting the availability of such connections impedes the adversary's ability to move freely through organizational systems.

Related Controls: SC-10.

References: None.

SI-15 INFORMATION OUTPUT FILTERING

Control: Validate information output from the following software programs and/or applications to ensure that the information is consistent with the expected content: [*Assignment: organization-defined software programs and/or applications*].

Discussion: Certain types of attacks, including SQL injections, produce output results that are unexpected or inconsistent with the output results that would be expected from software programs or applications. Information output filtering focuses on detecting extraneous content, preventing such extraneous content from being displayed, and then alerting monitoring tools that anomalous behavior has been discovered.

Related Controls: SI-3, SI-4, SI-11.

Control Enhancements: None.

References: None.

SI-16 MEMORY PROTECTION

Control: Implement the following controls to protect the system memory from unauthorized code execution: [*Assignment: organization-defined controls*].

Discussion: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data

execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

Related Controls: AC-25, SC-3, SI-7.

Control Enhancements: None.

References: None.

SI-17 FAIL-SAFE PROCEDURES

Control: Implement the indicated fail-safe procedures when the indicated failures occur: [*Assignment: organization-defined list of failure conditions and associated fail-safe procedures*].

Discussion: Failure conditions include the loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include alerting operator personnel and providing specific instructions on subsequent steps to take. Subsequent steps may include doing nothing, reestablishing system settings, shutting down processes, restarting the system, or contacting designated organizational personnel.

Related Controls: CP-12, CP-13, SC-24, SI-13.

Control Enhancements: None.

References: None.

SI-18 PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS

Control:

a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle [*Assignment: organization-defined frequency*]; and

b. Correct or delete inaccurate or outdated personally identifiable information.

Discussion: Personally identifiable information quality operations include the steps that organizations take to confirm the accuracy and relevance of personally identifiable information throughout the information life cycle. The information life cycle includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information. Personally identifiable information quality operations include editing and validating addresses as they are collected or entered into systems using automated address verification look-up application programming interfaces. Checking personally identifiable information quality includes the tracking of updates or changes to data over time, which enables organizations to know how and what personally identifiable information was changed should erroneous information be identified. The measures taken to protect personally identifiable information quality are based on the nature and context of the personally identifiable information, how it is to be used, how it was obtained, and the potential de-identification methods employed. The measures taken to validate the accuracy of personally identifiable information used to make determinations about the rights, benefits, or privileges of individuals covered under federal programs may be more comprehensive than the measures used to validate personally identifiable information used for less sensitive purposes.

Related Controls: PM-22, PM-24, PT-2, SI-4.

Control Enhancements:

(1) PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | AUTOMATION SUPPORT

Correct or delete personally identifiable information that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified using [*Assignment: organization-defined automated mechanisms*].

Discussion: The use of automated mechanisms to improve data quality may inadvertently create privacy risks. Automated tools may connect to external or otherwise unrelated systems, and the matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessments and make determinations that are in alignment with their privacy program plans.

As data is obtained and used across the information life cycle, it is important to confirm the accuracy and relevance of personally identifiable information. Automated mechanisms can augment existing data quality processes and procedures and enable an organization to better identify and manage personally identifiable information in large-scale systems. For example, automated tools can greatly improve efforts to consistently normalize data or identify malformed data. Automated tools can also be used to improve the auditing of data and detect errors that may incorrectly alter personally identifiable information or incorrectly associate such information with the wrong individual. Automated capabilities backstop processes and procedures at-scale and enable more fine-grained detection and correction of data quality errors.

Related Controls: PM-18, RA-8.

(2) PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | DATA TAGS

Employ data tags to automate the correction or deletion of personally identifiable information across the information life cycle within organizational systems.

Discussion: Data tagging personally identifiable information includes tags that note processing permissions, authority to process, de-identification, impact level, information life cycle stage, and retention or last updated dates. Employing data tags for personally identifiable information can support the use of automation tools to correct or delete relevant personally identifiable information.

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

(3) PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | COLLECTION

Collect personally identifiable information directly from the individual.

Discussion: Individuals or their designated representatives can be sources of correct personally identifiable information. Organizations consider contextual factors that may incentivize individuals to provide correct data versus false data. Additional steps may be necessary to validate collected information based on the nature and context of the personally identifiable information, how it is to be used, and how it was obtained. The measures taken to validate the accuracy of personally identifiable information used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than the measures taken to validate less sensitive personally identifiable information.

Related Controls: None.

(4) PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | INDIVIDUAL REQUESTS

Correct or delete personally identifiable information upon request by individuals or their designated representatives.

Discussion: Inaccurate personally identifiable information maintained by organizations may cause problems for individuals, especially in those business functions where inaccurate information may result in inappropriate decisions or the denial of benefits and services to individuals. Even correct information, in certain circumstances, can cause problems for

individuals that outweigh the benefits of an organization maintaining the information. Organizations use discretion when determining if personally identifiable information is to be corrected or deleted based on the scope of requests, the changes sought, the impact of the changes, and laws, regulations, and policies. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding appropriate instances of correction or deletion.

Related Controls: None.

(5) PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | NOTICE OF CORRECTION OR DELETION

Notify [*Assignment: organization-defined recipients of personally identifiable information*] and individuals that the personally identifiable information has been corrected or deleted.

Discussion: When personally identifiable information is corrected or deleted, organizations take steps to ensure that all authorized recipients of such information, and the individual with whom the information is associated or their designated representatives, are informed of the corrected or deleted information.

Related Controls: None.

References: [OMB M-19-15], [SP 800-188], [IR 8112].

SI-19 DE-IDENTIFICATION

Control:

a. Remove the following elements of personally identifiable information from datasets: [*Assignment: organization-defined elements of personally identifiable information*]; and

b. Evaluate [*Assignment: organization-defined frequency*] for effectiveness of de-identification.

Discussion: De-identification is the general term for the process of removing the association between a set of identifying data and the data subject. Many datasets contain information about individuals that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. Datasets may also contain other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Personally identifiable information is removed from datasets by trained individuals when such information is not (or no longer) necessary to satisfy the requirements envisioned for the data. For example, if the dataset is only used to produce aggregate statistics, the identifiers that are not needed for producing those statistics are removed. Removing identifiers improves privacy protection since information that is removed cannot be inadvertently disclosed or improperly used. Organizations may be subject to specific de-identification definitions or methods under applicable laws, regulations, or policies. Re-identification is a residual risk with de-identified data. Re-identification attacks can vary, including combining new datasets or other improvements in data analytics. Maintaining awareness of potential attacks and evaluating for the effectiveness of the de-identification over time support the management of this residual risk.

Related Controls: MP-6, PM-22, PM-23, PM-24, RA-2, SI-12.

Control Enhancements:

(1) DE-IDENTIFICATION | COLLECTION

De-identify the dataset upon collection by not collecting personally identifiable information.

Discussion: If a data source contains personally identifiable information but the information will not be used, the dataset can be de-identified when it is created by not collecting the

data elements that contain the personally identifiable information. For example, if an organization does not intend to use the social security number of an applicant, then application forms do not ask for a social security number.

Related Controls: None.

(2) DE-IDENTIFICATION | ARCHIVING

Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived.

Discussion: Datasets can be archived for many reasons. The envisioned purposes for the archived dataset are specified, and if personally identifiable information elements are not required, the elements are not archived. For example, social security numbers may have been collected for record linkage, but the archived dataset may include the required elements from the linked records. In this case, it is not necessary to archive the social security numbers.

Related Controls: None.

(3) DE-IDENTIFICATION | RELEASE

Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.

Discussion: Prior to releasing a dataset, a data custodian considers the intended uses of the dataset and determines if it is necessary to release personally identifiable information. If the personally identifiable information is not necessary, the information can be removed using de-identification techniques.

Related Controls: None.

(4) DE-IDENTIFICATION | REMOVAL, MASKING, ENCRYPTION, HASHING, OR REPLACEMENT OF DIRECT IDENTIFIERS

Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.

Discussion: There are many possible processes for removing direct identifiers from a dataset. Columns in a dataset that contain a direct identifier can be removed. In masking, the direct identifier is transformed into a repeating character, such as XXXXXX or 999999. Identifiers can be encrypted or hashed so that the linked records remain linked. In the case of encryption or hashing, algorithms are employed that require the use of a key, including the Advanced Encryption Standard or a Hash-based Message Authentication Code. Implementations may use the same key for all identifiers or use a different key for each identifier. Using a different key for each identifier provides a higher degree of security and privacy. Identifiers can alternatively be replaced with a keyword, including transforming "George Washington" to "PATIENT" or replacing it with a surrogate value, such as transforming "George Washington" to "Abraham Polk."

Related Controls: SC-12, SC-13.

(5) DE-IDENTIFICATION | STATISTICAL DISCLOSURE CONTROL

Manipulate numerical data, contingency tables, and statistical findings so that no individual or organization is identifiable in the results of the analysis.

Discussion: Many types of statistical analyses can result in the disclosure of information about individuals even if only summary information is provided. For example, if a school that publishes a monthly table with the number of minority students enrolled, reports that it has 10-19 such students in January, and subsequently reports that it has 20-29 such students in March, then it can be inferred that the student who enrolled in February was a minority.

Related Controls: None.

(6) DE-IDENTIFICATION | DIFFERENTIAL PRIVACY

Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported.

Discussion: The mathematical definition for differential privacy holds that the result of a dataset analysis should be approximately the same before and after the addition or removal of a single data record (which is assumed to be the data from a single individual). In its most basic form, differential privacy applies only to online query systems. However, it can also be used to produce machine-learning statistical classifiers and synthetic data. Differential privacy comes at the cost of decreased accuracy of results, forcing organizations to quantify the trade-off between privacy protection and the overall accuracy, usefulness, and utility of the de-identified dataset. Non-deterministic noise can include adding small, random values to the results of mathematical operations in dataset analysis.

Related Controls: SC-12, SC-13.

(7) DE-IDENTIFICATION | VALIDATED ALGORITHMS AND SOFTWARE

Perform de-identification using validated algorithms and software that is validated to implement the algorithms.

Discussion: Algorithms that appear to remove personally identifiable information from a dataset may in fact leave information that is personally identifiable or data that is re-identifiable. Software that is claimed to implement a validated algorithm may contain bugs or implement a different algorithm. Software may de-identify one type of data, such as integers, but not de-identify another type of data, such as floating point numbers. For these reasons, de-identification is performed using algorithms and software that are validated.

Related Controls: None.

(8) DE-IDENTIFICATION | MOTIVATED INTRUDER

Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.

Discussion: A motivated intruder test is a test in which an individual or group takes a data release and specified resources and attempts to re-identify one or more individuals in the de-identified dataset. Such tests specify the amount of inside knowledge, computational resources, financial resources, data, and skills that intruders possess to conduct the tests. A motivated intruder test can determine if the de-identification is insufficient. It can also be a useful diagnostic tool to assess if de-identification is likely to be sufficient. However, the test alone cannot prove that de-identification is sufficient.

Related Controls: None.

References: [OMB A-130], [SP 800-188].

SI-20 TAINTING

Control: Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: [*Assignment: organization-defined systems or system components*].

Discussion: Many cyber-attacks target organizational information, or information that the organization holds on behalf of other entities (e.g., personally identifiable information), and exfiltrate that data. In addition, insider attacks and erroneous user procedures can remove information from the system that is in violation of the organizational policies. Tainting approaches can range from passive to active. A passive tainting approach can be as simple as adding false email names and addresses to an internal database. If the organization receives email at one of the false email addresses, it knows that the database has been compromised. Moreover, the organization knows that the email was sent by an unauthorized entity, so any

packets it includes potentially contain malicious code, and that the unauthorized entity may have potentially obtained a copy of the database. Another tainting approach can include embedding false data or steganographic data in files to enable the data to be found via open-source analysis. Finally, an active tainting approach can include embedding software in the data that is able to "call home," thereby alerting the organization to its "capture," and possibly its location, and the path by which it was exfiltrated or removed.

Related Controls: AU-13.

Control Enhancements: None.

References: [OMB A-130], [SP 800-160-2].

SI-21 INFORMATION REFRESH

Control: Refresh [*Assignment: organization-defined information*] at [*Assignment: organization-defined frequencies*] or generate the information on demand and delete the information when no longer needed.

Discussion: Retaining information for longer than it is needed makes it an increasingly valuable and enticing target for adversaries. Keeping information available for the minimum period of time needed to support organizational missions or business functions reduces the opportunity for adversaries to compromise, capture, and exfiltrate that information.

Related Controls: SI-14.

Control Enhancements: None.

References: [OMB A-130], [SP 800-160-2].

SI-22 INFORMATION DIVERSITY

Control:

a. Identify the following alternative sources of information for [*Assignment: organization-defined essential functions and services*]: [*Assignment: organization-defined alternative information sources*]; and

b. Use an alternative information source for the execution of essential functions or services on [*Assignment: organization-defined systems or system components*] when the primary source of information is corrupted or unavailable.

Discussion: Actions taken by a system service or a function are often driven by the information it receives. Corruption, fabrication, modification, or deletion of that information could impact the ability of the service function to properly carry out its intended actions. By having multiple sources of input, the service or function can continue operation if one source is corrupted or no longer available. It is possible that the alternative sources of information may be less precise or less accurate than the primary source of information. But having such sub-optimal information sources may still provide a sufficient level of quality that the essential service or function can be carried out, even in a degraded or debilitated manner.

Related Controls: None.

Control Enhancements: None.

References: [SP 800-160-2].

SI-23 INFORMATION FRAGMENTATION

Control: Based on [*Assignment: organization-defined circumstances*]:

a. Fragment the following information: [*Assignment: organization-defined information*]; and

b. Distribute the fragmented information across the following systems or system components: [*Assignment organization-defined systems or system components*].

Discussion: One objective of the advanced persistent threat is to exfiltrate valuable information. Once exfiltrated, there is generally no way for the organization to recover the lost information. Therefore, organizations may consider dividing the information into disparate elements and distributing those elements across multiple systems or system components and locations. Such actions will increase the adversary's work factor to capture and exfiltrate the desired information and, in so doing, increase the probability of detection. The fragmentation of information impacts the organization's ability to access the information in a timely manner. The extent of the fragmentation is dictated by the impact or classification level (and value) of the information, threat intelligence information received, and whether data tainting is used (i.e., data tainting-derived information about the exfiltration of some information could result in the fragmentation of the remaining information).

Related Controls: None.

Control Enhancements: None.

References: [SP 800-160-2].