**System and Information Integrity (SI)**

**SI-1: System and Information Integrity Policy and Procedures**

NIST SP 800-53 Objective: The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

b. Reviews and updates the current:

1. System and information integrity policy [Assignment: organization-defined frequency]; and

2. System and information integrity procedures [Assignment: organization-defined frequency].

Control Translation: Ensure System and Information Integrity policy and procedures are in place.

Notes: The organizational risk management strategy is a key factor in the development of the system and information integrity policy. Related control: PM-9. This control can be applied at the General level.

How to test and evaluate: Examine SSP and System Information and Integrity Policy (if available). Verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency.

Technology specific: General

**SI-2: Flaw Remediation**

NIST SP 800-53 Objective: The organization:

a. Identifies, reports, and corrects information system flaws;

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

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

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

Control Translation: Ensure System and Information Integrity policy and procedures have flaw remediation mechanism in place.

Notes: Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems.

Notes: By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.

How to test and evaluate: Examine SSP and System Information and Integrity Policy (if available) and verify that the policy and procedures indicate that flaw remediation is in place and that it is incorporated with ongoing configuration management process. Ensure organization identifies, reports, and corrects information system flaws. Also verify that software tests and firmware updates are documented and if there are automated mechanisms used for flaw remediation.

Technology specific: All

**SI-3: Malicious Code Protection**

NIST SP 800-53 Objective: The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

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

c. Configures malicious code protection mechanisms to:

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

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

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

Control Translation: Ensure System and Information Integrity policy and procedures have malicious code protection in place.

Notes: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.

Notes: 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, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

How to test and evaluate: Examine SSP and System Information and Integrity Policy (if available) and verify that the policy and procedures indicate that malicious code protection mechanisms are in place. Note where are the protection mechanisms placed (e.g., at entry and exit points of network) and if real-time detection is occurring. Indicate whether malicious code is blocked, quarantined, and if alert is sent to administrator. Verify if malicious code protection mechanisms are updated whenever new releases are available and if updates are automated. If not, what type of updating process is implemented at organization.

Technology specific: All

**SI-4: Information System Monitoring**

NIST SP 800-53 Objective: The organization:

a. Monitors the information system to detect:

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

2. Unauthorized local, network, and remote connections;

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

c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

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

Control Translation: Ensure System and Information Integrity policy and procedures have information system monitoring in place.

Notes: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, 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 may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17.

Notes: Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

How to test and evaluate: Examine SSP and System Information and Integrity Policy (if available) and verify that the policy and procedures indicate that information system monitoring is in place. Note what type of network monitoring devices are deployed, if remote connection is allowed, if intrusion-monitoring tools are used to protect information from unauthorized access, modification, and deletion, and what roles have access to monitoring devices.

Technology specific: All

**SI-5: Security Alerts, Advisories, and Directives**

NIST SP 800-53 Objective: The organization:

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

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

c. Disseminates 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. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Control Translation: Ensure System and Information Integrity policy and procedures have system alerts, advisories and directives in place.

Notes: The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to 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.

Notes: External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations. Related control: SI-2.

How to test and evaluate: Examine SSP and System Information and Integrity Policy (if available) and verify that the policy and procedures indicate that system alerts, advisories, and directives are in place. Note from where does organization receive information system security alerts, advisories, and directives. Verify if internal alerts are generated , from personnel/team/role generates the alerts and if alerts are generated in real-time.

Technology specific: All

**SI-6: Security Function Verification**

NIST SP 800-53 Objective: The organization:

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

b. Performs this verification [*Selection (one or more):* [*Assignment: organization-defined system transitional states*]*; upon command by user with appropriate privilege;* [*Assignment: organization-defined frequency*]];

c. Notifies [*Assignment: organization-defined personnel or roles*] of failed security verification tests; and

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

Control Translation: Ensure System and Information Integrity policy and procedures have security function verification checks in place.

Notes: Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights. Related controls: CA-7, CM-6.

How to test and evaluate: Examine SSP and System Information and Integrity Policy (if available) and verify that the policy and procedures indicate that security function verification is in place. Note how verification checks are performed and who has privilege to perform the checks. Also note who is notified if security verification tests fail. Verify if system will shut down or restart when anomalies are discovered.

Technology specific: All

**SI-7: Software, Firmware, and Information Integrity**

NIST SP 800-53 Objective: The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*].

Control Translation: Ensure System and Information Integrity policy and procedures states that organization employs integrity verification/integrity checking mechanisms and tools to detect unauthorized changes to software, firmware, and information.

Notes: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3.

How to test and evaluate: Examine SSP and System Information and Integrity Policy (if available) and verify that the policy and procedures indicate that organization employs integrity verification/integrity checking mechanisms and tools to detect unauthorized changes to software, firmware, and information. Note what tools/mechanisms are used and if it is automated.

Technology specific: All

**SI-8: Spam Protection**

NIST SP 800-53 Objective: The organization:

a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and

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

Control Translation: Ensure System and Information Integrity policy and procedures states that spam protection mechanism is in place.

Notes: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions. Related controls: AT-2, AT-3, SC-5, SC-7, SI-3.

How to test and evaluate: Examine SSP and System Information and Integrity Policy (if available) and verify that the policy and procedures indicate that organization employs spam protection mechanism. Note what spam tool is used and where is it implemented at entry and exit points of organization network.

Technology specific: General

**SI-10: Information Input Validation**

NIST SP 800-53 Objective: The information system checks the validity of [*Assignment: organization-defined information inputs*].

Control Translation: Ensure System and Information Integrity policy and procedures states that information input validation mechanism is in place.

Notes: Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software 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 tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

How to test and evaluate: Examine SSP and System Information and Integrity Policy (if available) and verify that the policy and procedures indicate that organization employs information input validation mechanism. Note what tools/software is used in checking the validity of input to ensure accurate and correct inputs to prevent attacks (e.g., cross-site scripting, injection attacks, definition checks such as character set, length, values, etc.)

Technology specific: All

**SI-11: Error Handling**

NIST SP 800-53 Objective: The information system:

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

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

Control Translation: Ensure System and Information Integrity policy and procedures states that error handling mechanism is in place.

Notes: Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information. Related controls: AU-2, AU-3, SC-31.

How to test and evaluate: Examine SSP and System Information and Integrity Policy (if available) and verify that the policy and procedures indicate that organization employs error handling mechanism. Note if error message is generated for corrective action without revealing information and indicate who handles these errors. Obtain samples of error messages generated by the component

Technology specific: All

**SI-12: Information Handling and Retention**

NIST SP 800-53 Objective: The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Control Translation: Ensure System and Information Integrity policy and procedures states that information handling and retention mechanism is in place.

Notes: Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4.

How to test and evaluate: Examine SSP and System Information and Integrity Policy (if available) and verify that the policy and procedures indicate that organization employs information handling and retention mechanism. Note how long information is retained for and how information is archived or disposed of.

Technology specific: General

**SI-16: Memory Protection**

NIST SP 800-53 Objective: The information system implements [*Assignment: organization-defined security safeguards*] to protect its memory from unauthorized code execution.

Control Translation: Ensure System and Information Integrity policy and procedures states that memory protection is in place.

Notes: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism. Related controls: AC-25, SC-3.

How to test and evaluate: Examine SSP and System Information and Integrity Policy (if available) and verify that the policy and procedures indicate that organization employs safeguards to protect memory from unauthorized code execution. Note what safeguard is in place and validate its implementation.

Technology specific: All