Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – System and Information Integrity (SI) Procedure

1. PURPOSE

The Environmental Protection Agency (EPA) is responsible for ensuring all offices within the Agency meet the minimum-security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems shall meet the security requirements by implementing the security controls defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

The purpose of this procedure is to facilitate the implementation of the EPA security control requirements for the System and Information Integrity (SI) control family, as identified in NIST SP 800-53, Revision 5.

2. SCOPE

These procedures address all EPA information and information systems to include information and information systems used, managed or operated by a contractor, another agency or other organization on behalf of the EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. AUTHORITY

- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)
- Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource," July 2016
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020

5. PROCEDURE

SIO, ISO and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system through a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide, and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and EPA SO or their official designees and SM for the systems that they oversee.

The "SI" designator (e.g., SI-2, SI-3) identified for each procedure below corresponds to the NIST- identifier for the System and Information Integrity control family, as identified in NIST SP 800-53, Revision 5.

NIST defines the applicable SI security and privacy baseline controls in NIST 800-53B, *Control Baselines for Information Systems and Organizations*. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name. EPA may deviate from the NIST 800-53B Security or Privacy Control Baselines by adding/removing controls or to applicable baselines and are notated with an asterisk.

SI-2 – Flaw Remediation

For All Systems:

1) Identify, report and correct system flaws;
2) Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3) Install security-relevant software and firmware within the following timelines:
   a) **Critical**- within fifteen (15) calendar days;
   b) **Cybersecurity and Infrastructure Security Agency (CISA) – defined Known Exploited Vulnerabilities** – as defined within the catalog;
   c) **High Vulnerabilities** – within thirty (30) calendar days;
   d) **Moderate Vulnerabilities** – within sixty (60) calendar days;
   e) **Low Vulnerabilities** – ninety (90) calendar days;
   f) **Other** – Timelines may be reduced when directed by management, federal mandates (e.g. Binding Operational Directive (BOD), Cybersecurity Coordination, Assessment, and Response (CCAR)), and when threat or risk conditions warrant adjustments of the release of the updates; and
4) Incorporate flaw remediation into the organizational configuration management process.

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

For Moderate and High Systems:

1) Determine if system components have applicable security-relevant software and firmware updates installed using the EPA Enterprise approved patch management

and vulnerability scanning tools to scan software and hardware assets at least every 72 hours.

SI-3 – Malicious Code Protection

For All Systems:

1) Implement signature based and/or non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;
2) Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
3) Configure malicious code protection mechanisms to:
   a) Perform periodic scans of the system daily and real-time scans of files from external sources at endpoint, network entry and exit points as the files are downloaded, opened or executed in accordance with organizational policy; and
   b) Block malicious code or quarantine malicious code automatically, and send alerts to the Computer Security Incident Response Capability (CSIRC), System Administrators (SA), ISO, SM and/or other staff designated by the SO in response to malicious code detection; and
4) Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

SI-4 – System Monitoring

For All Systems:

1) Monitor the system to detect:
   a) Attacks and indicators of potential attacks in accordance with the following monitoring objectives: reduce the frequency of attacks, reduce the impact of attacks and deter potential attacks*;* and
   b) Unauthorized local, network and remote connections;
2) Identify unauthorized use of the system through the following techniques and methods: deployment, monitoring, correlation, and/or analysis of intrusion detection and prevention systems; malicious code protection software, network monitoring tools, user behavior analysis, data loss prevention, and enterprise audit log capturing, monitoring and analysis tools;
3) Invoke internal monitoring capabilities or deploy monitoring devices:
   a) Strategically within the system to collect organization-determined essential information; and
   b) At ad hoc locations within the system to track specific types of transactions of interest to the organization;
4) Analyze detected events and anomalies;
5) 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;
6) Obtain legal opinion regarding system monitoring activities; and
7) Provide information system, security event, user activity, and incident data as required to support cybersecurity investigations and incident response activities to CSIRC, SM, ISO and/or others designated by the SO as needed to support EPA's information security objectives.

SI-4(2) – System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis

For Moderate and High Systems:

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

SI-4(4) – System Monitoring | Inbound and Outbound Communications Traffic

For Moderate and High Systems:

1) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; and
2) Monitor inbound and outbound communications traffic continuously for indications of malicious code, unauthorized use of legitimate code or other evidence of potential compromise to the system or system components.

SI-4(5) – System Monitoring | System-generated Alerts

For Moderate and High Systems:

1) Alert SA, CSIRC, ISO, SM, and others as designated when the following system-generated indications of compromise or potential compromise occur:
   a) Audit alerts from enterprise security information and event management (SIEM) or log management tools to include system, application and security logs;
   b) Input from malicious code protection mechanisms;
   c) Intrusion detection and prevention mechanisms; and
   d) Boundary protection devices, such as firewalls, gateways and routers.

SI-4(10) – System Monitoring | Visibility of Encrypted Communications

For High Systems:

1) Make provisions so that encrypted traffic entering/exiting a perimeter and encrypted e-mail traffic is visible to data loss prevention (DLP), enterprise SIEM log management or other monitoring tools.

SI-4(12) – System Monitoring | Automated Organization-Generated Alerts

For High Systems:

1) Alert SA, CSIRC, ISO, SM, and others as designated using automated systems when the following indications of inappropriate or unusual activities with security or privacy implications occur: indications of compromise or potential compromise listed in SI-4(5).

SI-4(14) – System Monitoring | Wireless Intrusion Detection

For High Systems:

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

SI-4(20) – System Monitoring | Privileged Users

For High Systems:

1) Implement the following additional monitoring of privileged users: consistent with the audit and accountability (AU) control requirements.

SI-4(22) – System Monitoring | Unauthorized Network Services
For High Systems:
1) Detect network services that have not been authorized or approved by the SO, SIO, SM, or ISO; and
2) Alert the SA, CSIRC, ISO, SM, and others as designated when detected.

SI-5 – Security Alerts, Advisories and Directives
For All Systems:
1) Receive system security alerts, advisories, and directives from DHS, other Federal Agencies (i.e., FBI, NSA, OMB), vendors, developers, and other trusted third-parties sources on an ongoing basis;
2) Generate internal security alerts, advisories, and directives as deemed necessary;
3) Disseminate security alerts, advisories and, directives to the SAs, CSIRC, ISO, ISSO, SO, IMO, and SIO, key security personnel and the EPA Patch Management Teams; and
4) Implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.

SI-5(1) – Security Alerts, Advisories and Directives | Automated Alerts and Advisories
For High Systems:
1) Broadcast security alert and advisory information throughout the organization using approved communication methods such as mass mailers, SharePoint sites, and targeted email messages via pre-defined distribution lists.

SI-6 – Security Function Verification
For High Systems:
1) Verify the correct operation of all applicable security and privacy functions;
2) Perform the verification of the functions specified in SI-6 1) at the following transition states: during startup; restarts; shutdowns; and aborts; upon command by user with appropriate privilege; and at least quarterly;
3) Alert the SA, CSIRC, ISO, SM, and others as designated to failed security and privacy verification tests; and
4) Shut the system down, restart the system or implement system-defined actions when anomalies are discovered.

SI-7 – Software, Firmware and Information Integrity
For Moderate and High Systems:
1) Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: configuration baselines; authorized software; system-specified Controlled Unclassified Information (CUI) information types; and
2) Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify SA, CSIRC, ISO, SM, and others as designated.

SI-7(1) – Software, Firmware, and Information Integrity | Integrity Checks
For Moderate and High Systems:
1) Perform an integrity check of software, firmware and information at startup, during transitional states and/or occurrence of security related events including the identification of new threats to which systems may be susceptible and installation of new hardware, software, or firmware and on a quarterly basis.

SI-7(2) – Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations

For High Systems:

1) Employ automated tools that provide notification to SA, CSIRC, ISO, SM, and others as designated upon discovering discrepancies during integrity verification.

SI-7(5) – Software, Firmware, and Information Integrity | Automated Response to Integrity Violations

For High Systems:

1) Automatically shut the system down, restart the system or implement system-defined actions when integrity violations are discovered.

SI-7(7) - Software, Firmware, and Information Integrity | Integration of Detection and Response

For Moderate and High Systems:

1) Incorporate the detection of the following unauthorized changes into the organizational incident response capability: operating system, software, established configuration settings and elevation of system privileges.

SI-7(15) – Software, Firmware, and Information Integrity | Code Authentication

For High Systems:

1) Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: baseline images, new approved software/firmware, code changes as applicable, updates/patches.

SI-8 – Spam Protection

For Moderate and High Systems:

1) Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and
2) Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

SI-8(2) – Spam Protection | Automatic Updates

For Moderate and High Systems:

1) Automatically update spam protection mechanisms when updates are made available.

SI-10 – Information Input Validation

For Moderate and High Systems:

1) Check the validity of the following information inputs: all arguments or input data strings submitted by manual or automated processes.

SI-11 – Error Handling

For Moderate and High Systems:

1) Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and
2) Reveal error messages only to authorized personnel (e.g., systems administrators, maintenance personnel).

SI-12 – Information Management and Retention
For All Systems and Privacy Control Baseline:
1) 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.

SI-12(1) – Information Management and Retention | Limit Personally Identifiable Information Elements
For Privacy Control Baseline:
1) Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information as defined by the Privacy Act of 1974.

SI-12(2) – Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research
For Privacy Control Baseline:
1) Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: live production data shall not be used for research, testing or training. Only fake or dummy data may be used for these purposes.

SI-12(3) – Information Management and Retention | Informal Disposal
For Privacy Control Baseline:
1) Use the following techniques to dispose of, destroy, or erase information following the retention period: defined in the Information Security - Media Protection Procedures.

SI-16 – Memory Protection
For Moderate and High Systems:
1) Implement the following controls to protect the system memory from unauthorized code execution: EPA approved security measures, commensurate with the information system’s sensitivity level, to include but not limited to either hardware or software enforced data execution prevention and address space layout randomization.

SI-18 – Personally Identifiable Information Quality Operations
For Privacy Control Baseline:
1) Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle annually or when new data types are being utilized; and
2) Correct or delete inaccurate or outdated personally identifiable information.

SI-18(4) – Personally Identifiable Information Quality Operations | Individual Requests
For Privacy Control Baseline:
1) Correct or delete personally identifiable information upon request by individuals or their designated representatives.

SI-19 – De-identification
For Privacy Control Baseline:

1) Remove the following elements of personally identifiable information from datasets: any elements about individuals that can be used to distinguish or trace an individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records**;** any information that is linked or linkable to an individual e.g., protected health information (PHI), educational, financial, and employment information; and
2) Evaluate within two (2) weeks for effectiveness of de-identification.

6. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

7. RELATED INFORMATION

- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

8. DEFINITIONS

- **External Monitoring** - the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection).
- **Incident/Security Incident** - an occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.
- **Information** - any communication or representation of knowledge such as facts, data or opinions in any medium, including paper and electronic, or form, including textual, numerical, graphic, cartographic, narrative or audiovisual.
- **Information System** - a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.
- **Internal Monitoring** - the observation of events occurring within the system (e.g., within internal organizational networks and system components).
- **Malicious Code** - software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity or availability of an information system. A virus, worm, Trojan horse or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
- **Media** - physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, printouts (but not display media) onto which information is recorded, stored or printed within an information system. Digital media include diskettes, tapes,

removable hard drives, flash/thumb drives, compact discs and digital video discs. Examples of non-digital media are paper or microfilm. This term also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

- **Personally Identifiable Information (PII)** - any information about an individual maintained by an agency that can be used to distinguish, trace or identify an individual's identity, including personal information which is linked or linkable to an individual. Examples of PII include name, social security number, date and place of birth, mother's maiden name, or biometric records and (2) any other information that is linked or linkable to an individual, e.g., PHI, educational, financial and employment information.
- **Privacy Act Information** - data about an individual that is retrieved by name or another personal identifier assigned to the individual.
- **Records** - the recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results) which serve as the basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
- **Risk** - a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
- **Signature** (of an individual) - a mark or sign made by an individual to signify knowledge, approval, acceptance or obligation (can be accomplished manually, sometimes referred to as a "wet signature," or electronically).
- **Spyware -** software that is secretly installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
- **Threat** - any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image or reputation), agency assets or individuals through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.
- **Vulnerability** - weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
- **Written** (or in writing) - means to officially document the action or decision, either manually or electronically and including a signature.

9. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

10. DIRECTIVE(S) SUPERSEDED

This procedure supersedes Information Directive: CIO 2150-P-17.2, Information Security – System and Information Integrity Procedures, January 17, 2017.

11. CONTACTS

For information about this directive, please contact the Office of Mission Support (OMS), Office of Information Security and Privacy (OISP) at Infosec@epa.gov.

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2023.11.21 14:11:51 -05'00'

Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Information Technology and Information Management

APPENDIX A: ACRONYMS & ABBREVIATIONS

BOD	Binding Operational Directive
CCAR	Cybersecurity Coordination, Assessment, and Response
CISA	Cybersecurity and Infrastructure Security Agency
CSIRC	Computer Security Incident Response Capability
CUI	Controlled Unclassified Information
DLP	data loss prevention
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization
ISO	Information Security Officers
NHS	National Health Services
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OISP	Office of Information Security and Privacy
OMB	Office of Management and Budget
OMS	Office of Mission Support
PHI	Protected Health Information
PII	Personally Identifiable Information
SA	System Administrators
SI	System and Information Integrity
SIEM	Security information and event management
SIO	Senior Information Officials
SM	Service Managers
SO	System Owners
SP	Special Publication
U.S.C.	United States Code