EPA

INFORMATION DIRECTIVE
INTERIM PROCEDURE

Information Security – Interim System and Information Integrity Procedures		
Directive No.: 2150-P-17.2	CIO Approval: 1/17/2017	Transmittal No.:17-006

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

Information Security – Interim System and Information Integrity Procedures

1. PURPOSE

To extend and provide specificity to the Environmental Protection Agency (EPA) Information Security Policy. This document shall be used to develop procedures, standards and guidance that facilitate the implementation of security control requirements for the System and Information Integrity (SI) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

2. SCOPE

The procedures cover 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.

The procedures apply to all EPA employees, contractors and all other users of EPA information and information systems that support the operation and assets of the EPA.

3. AUDIENCE

The audience is all EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA.

4. BACKGROUND

Based on federal requirements and mandates, the 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 through the use of the security controls defined in NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. This document addresses the procedures and standards set forth by the EPA, and complies with the System and Information Integrity (SI) family of controls.

5. AUTHORITY

- Cybersecurity Act of 2015, Public Law 114-113

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act (FISMA), as amended
- Federal Information Security Modernization (FISMA) Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3519)
- Privacy Act of 1974 (5 U.S.C. § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—“Employees Responsible for the Management or Use of Federal Computer Systems,” Section 930.301 through 930.305 (5 C.F.R. 930.301-305)
- Office of Management and Budget (OMB) Memorandum M-02-01, “Guidance for Preparing and Submitting Security Plans of Action and Milestones,” October 2001
- OMB Memorandum M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,” September 2003
- OMB Memorandum M-06-16, “Protection of Sensitive Agency Information,” June 2006
- OMB Circular A-130, “Management of Federal Information Resources”, Appendix III, “Security of Federal Automated Information Resources,” July 2016
- Federal Information Processing Standards (FIPS) 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004
- FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006
- National Archives and Records Administration, 36 C.F.R. Chapter XII, Subchapter B - Records Management (Parts 1220-1238)
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA Information Security Continuous Monitoring Strategic Plan
- CIO Policy Framework and Numbering System

6. PROCEDURE

The "SI" designator identified in each procedure represents the NIST-specified identifier for the System and Information Integrity control family, as identified in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

SI-1 – System and Information Integrity Policy and Procedures

For All Information Systems:

1) The Director of Office of Information Technology Operations (OITO), in coordination with System Owners (SOs), Information Security Officers (ISOs), Information Owners (IOs), Information Management Officers (IMOs), and Information System Security Officers (ISSOs) shall; and Service Managers (SMs), in coordination with ISOs, IOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Develop, document, and disseminate to all EPA employees, contractors and other users of EPA systems:

i) A system and information integrity policy which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(1) Policies shall be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance where applicable.

ii) Procedures to facilitate the implementation of the system and information integrity and associated system and information integrity controls.

(1) Procedures shall be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance where applicable.

b) Review and update the current:

i) System and information integrity policy annually; and

ii) System and information integrity procedures annually.

For Federal Risk and Authorization Management Program (FedRAMP[1]) Low and Moderate Information Systems:

1) SMs, in coordination with ISOs, IOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Review and update the current:

i) System and information integrity policy at least every 3 years; and

ii) System and information integrity procedures at least annually.

For FedRAMP High Information Systems:

1) SMs, in coordination with ISOs, IOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Review and update the current:

i) System and information integrity policy at least annually; and

ii) System and information integrity procedure at least annually.

<u>SI-2 – Flaw Remediation</u>

[1] The FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.

For All Information Systems:

1) The Computer Security Incident Response Capability (CSIRC), for EPA-operated systems, shall; and SMs, in coordination with IOs and the CSIRC, for systems operated on behalf of the EPA, shall ensure service providers:

a) Develop and implement a capability[2] to identify, through Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) reporting sources, potential system flaws[3] and report them to SOs, ISOs, ISSOs and others for remediation and tracking.

b) Monitor the following by subscription, where available:

i) United States Computer Emergency Readiness Team (US-CERT) National Cyber Awareness System.

ii) National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD).

iii) Vendor and developer sites.

iv) Other third-party alert systems.

c) Produce notifications[4] for vulnerabilities and remediation containing instructions on how to apply them, if automated mechanisms are not used.

d) Configure, wherever practical and possible, operating systems and applications for EPA information systems and mobile devices to perform automatic updates (e.g., without administrator/operator intervention) in order to quickly remedy vulnerabilities and critical security issues as soon as updates become available.

Note: Due to information system integrity and availability concerns, organizations should give careful consideration to the methodologies used to perform automatic updates. Organizations shall balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and with any mission or operational impacts that automatic updates might impose.

i) Automatic updates shall be pre-approved for all critical systems and applications.

ii) To prevent spoofing and session hijacking, automatic updates shall be performed using only secure, EPA-approved methods and protocols (e.g., TLS 1.1, 1.2 and Hypertext Transfer Protocol Secure (HTTPS)).

iii) Automatically updating programs and operating systems shall be configured to notify system administrators/operators whenever automatic updates are performed.

[2] *CSIRC will monitor for security flaws and critical system threats and communicate them to the security community as they arise. CSIRC is not responsible for ensuring patches are applied or the tracking of the remediation, that is the responsibility of the System Owners.*

[3] *Flaws include errors in software, as well as errors in configuration settings for information systems. Flaw remediation encompasses installing software patches, service packs and hot fixes, as well as making changes to configuration settings. Vulnerability mitigation can also involve removing software or disabling functions, ports, protocols and/or services.*

[4] *CSIRC sends out vulnerability alerts that include, if known, remediation activities. These alerts are 'informational' in nature and do not necessarily include all applications or OS in use at the EPA. This would be the responsibility of the System Owner.*

2) SOs, in coordination with the EPA Patch Management Team, ISOs, Information Management Officers (IMO), SMs, IOs, ISSOs, Common Control Providers (CCP) and Security Control Assessors (SCA), for EPA-operated systems, shall; and SMs, in coordination with the EPA Patch Management Team, IOs, IMOs and ISOs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Ensure the latest patches and versions are used and installed for current and new devices in inventory in accordance with the following sites and communication from CSIRC:
        i) US-CERT National Cyber Alert System.
        ii) NIST NVD.
        iii) Vendor and developer sites.
        iv) Other third-party sites.
    b) Prioritize vulnerabilities and remediation actions based on the individual vulnerability criticality or severity ratings.
    c) Establish priorities based on the source’s assessment of severity or criticality as high, moderate, or low. The following sources (in order) shall be used unless the Senior Agency Information Security Officer (SAISO) establishes a different priority based on the most recent version of NIST’s NVD Common Vulnerability Scoring System (CVSS) Version 2.0 calculator.
        i) US-CERT’s established criticality.
        ii) Vendor web sites and mailing lists.
        iii) Third-party web sites.
        iv) Vulnerability scanner.
        v) Vulnerability databases.
        vi) Enterprise patch management tools.
        vii) Other notification tools.
    d) Modify, document and retain, as necessary, source severity assessments (other than those established by US-CERT) in accordance with detailed knowledge of criteria specific to the EPA by using NVD CVSS Version 2.0 calculator provided the criteria, ratings and results are documented and retained for the record and the alteration is noted in the alert.
        i) NVD’s CVSS Version 2.0 calculator shall be used to establish priority as follows:
            (a) Vulnerabilities shall be labeled "Low" severity if they have a CVSS base score of 0.0–3.9.
            (b) Vulnerabilities shall be labeled "Medium" severity if they have a base CVSS score of 4.0–6.9.
            (c) Vulnerabilities shall be labeled "High" or “Critical” severity if they have a CVSS base score of 7.0–10.0.
    e) Report flaws to the SAISO through the Plan of Actions and Milestones (POA&M) process via the Agency’s Federal Information Security Modernization Act (FISMA) reporting and tracking tool.

i) IOs and SMs shall obtain POA&Ms for systems operated on behalf of the EPA based on approved contracts and Service-Level Agreements (SLA) between the EPA and the service provider.

f) Manage flaw remediation through the POA&M process via the Agency's FISMA reporting and tracking tool.[5]

3) The SAISO, in coordination with the EPA Patch Management Team, SOs, ISOs, SMs, IOs and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with the EPA Patch Management Team, IOs, IMOs and ISOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Incorporate a Patch and Vulnerability Management Plan and flaw remediation into EPA's configuration management plan and processes.

4) The Director of OITO, in coordination with the EPA Patch Management Team, SOs, ISOs, IMOs, ISSOs, SMs and CCPs, for EPA-operated systems, shall; and SMs, in coordination with the EPA Patch Management Team, IOs, ISOs, IMOs and ISOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Develop and maintain configuration management plans or relevant documentation for all equipment, operating systems and software applications to contain the following:

i) The criteria for implementing flaw remediation with respect to threat levels, risk of compromise and consequences of compromise.

ii) The designated person responsible for monitoring and coordinating with each vendor for patch release support.

iii) The person responsible for testing patches.

iv) The process for installing patches in order to comply with the configuration management plan.

5) SOs, in coordination with the EPA Patch Management Team, ISOs, IMOs, ISSOs, SMs, CCPs and SCAs, for EPA-operated systems, shall; and SMs, in coordination with the EPA Patch Management Team, IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Use current change management procedures for testing low priority remediation and, when possible, for testing patches and configuration modifications of moderate priority vulnerabilities.

6) The EPA Patch Management Team and information security personnel shall:

a) Verify the software code for all patches, service packs, hot fixes, etc., before testing or installation.

i) A vendor authentication mechanism (e.g., cryptographic checksums, Pretty Good Privacy (PGP) signatures, digital certificates) shall be used to ensure the authenticity of the code.

ii) Secure Hash Algorithm-2 (SHA-2) checksums from vendors shall be used, instead of Message Digest Algorithm 5 (MD5) or similar checksums, when available.

[5] *Flaws may be discovered during security assessments, continuous monitoring, incident response and other activities.*

iii) The code shall be scanned for viruses using the most current virus signature database.

(1) A search shall be performed to learn what experiences others have had in installing or using the patch.

iv) All remediation changes shall be tested on non-production systems prior to implementation on any of EPA-standard Information Technology (IT) products and configured to reduce or eliminate the following:

(1) Unintended consequences.

(2) Alteration of security settings.

(3) Enabling default user accounts that had been disabled.

(4) Resetting default passwords for user accounts.

(5) Enabling services and functions that had been disabled.

(6) Non-security changes, such as new functionality.

(7) Introducing new vulnerabilities with a higher CVE score.

v) Patches shall be installed in the required sequence and tested to ensure previous security patches are not unintentionally removed.

(1) Testing shall include checking all related software and services to ensure they are operating correctly and as intended.

(2) Perform testing on designated systems identified for development or testing and accurately represent the current configuration of the systems in production to which the patch(es) will be applied.

(3) Conduct remediation testing on IT components that use current standard configurations or on virtual machines that contain the image of the current standard configurations.

7) SOs, in coordination with ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Obtain approval or request a waiver from the Chief Information Officer (CIO) for the use of non-standard IT products within the Agency.

b) Ensure that non-standard IT products undergo functionality and security testing using approved configuration standards.

i) Based on the test results, consider whether any significant disadvantages outweigh the benefits of installing a patch and determine whether remediation should be delayed.

(1) If potential negative consequences are significant, then the following shall be considered:

(a) Waiting until the vendor releases a newer patch that corrects the major issues.

(b) The ability to “undo” or uninstall a patch.

(c) Delaying high or moderate/medium priority remediation shall be approved by the SAISO with appropriate documentation of rationale and mitigation measures.

8) The EPA Patch Management Team and information security personnel shall:

a) Test security-relevant software and firmware updates related to flaw remediation, (including patches, service packs and hot fixes) prior to installation on EPA information systems, for effectiveness and potential side effects.

9) The Director of OITO, in coordination the EPA Patch Management Team, SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with the EPA Patch Management Team, IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Develop a schedule for the release and implementation of patches, service packs and hot fixes for Agency-standard configurations as needed and ensure the following:

i) The patch release schedule shall be developed using a risk-based decision that complies with pre-defined criteria (e.g., threat level, risk of compromise and consequences of compromise) outlined in the Patch and Vulnerability Management Plan.

ii) Security-relevant software updates (e.g., patches, service packs and hot fixes) shall be installed promptly by the EPA and EPA contractors.

iii) The requirements for testing and consideration of significant negative consequences if the remediation shall be applied.

iv) Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling shall be addressed expeditiously.

v) The priority of the vulnerability determines how promptly the remediation is implemented.

(a) Vulnerabilities ranked as “High” or “Critical” shall be mitigated and reported to CSIRC within 2 calendar days (48 Hours).

(b) Vulnerabilities ranked as “Moderate” shall be mitigated and reported to CSIRC within 7 calendar days.

(c) Vulnerabilities ranked as “Low” shall be mitigated and reported to CSIRC within 30 calendar days.

b) Confirm the automated deployment of patches to IT devices using EPA authorized automated patch management tools are used.

i) When automated mechanisms are not available, feasible, or appropriate, manual patch installation and remediation shall be performed.

c) Ensure automated tools acquired to support vulnerability and configuration management remediation actions are selected based on the following order of priority:

i) Tools that implement, support and are validated by NIST to conform to the Security Content Automation Protocol (SCAP).

ii) Tools that are pursuing or have a corporate commitment to conform to NIST validation of SCAP.

iii) Tools that readily integrate with other SCAP-validated tools.

iv) Commercial tools that lack SCAP validation, in the absence of validated tools.

v) Tools developed in house that readily integrate with SCAP-validated tools.

vi) Vulnerability and flaw remediation actions are tracked and verified.

vii) Appropriate automated tools and methods include, but are not limited to, the following:

(1) Patch deployment tool database.

(2) Network and host vulnerability scanning.

(3) Configuration management tool.

10) SOs, in coordination with ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Guarantee that when automated tools are not feasible, installation shall be verified by manual methods and supported with documented evidence; including, but not limited to the following:

i) Inspecting the configuration by, for example, viewing the Basic Input/Output System (BIOS) boot screen, “Help – About” or other available and appropriate verification mechanism for the hardware, operating system, or application.

ii) Reviewing files or configuration settings that the remediation was intended to correct to ensure that they have been changed as stated in the vendor’s documentation or instructions.

iii) Reviewing patch logs.

Note: Verification shall not employ exploit procedures (e.g., a penetration test) or code to exploit any vulnerabilities within a production environment without written authorization and approval from the information system’s Authorizing Official (AO). Exploit methods such as penetration testing may be used without authorization and approval only on test systems in a test environment.

b) Verify the completion of procedures contained in US-CERT guidance and Information Assurance Vulnerability Alerts.

c) Ensure, upon completion of flaw remediation and vulnerability mitigation activities, that the following actions occur:

i) The inventory of information systems and components shall be updated to reflect current software versions and configurations.

ii) Stakeholders, including but not limited to EPA’s CSIRC, shall be notified.

d) Report to CSIRC via the Agency incident reporting system and provide necessary evidence upon request, unless the status is available through an automated tool visible to CSIRC personnel.

For All FedRAMP Information Systems:

1) SMs, in coordination with ISOs, IOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Installs security-relevant software and firmware updates within 30 days of the release of the updates.

SI-2 (1) – Flaw Remediation | Central Management

For High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and CCPs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Manage the flaw remediation process centrally and configure the system to install software updates automatically, wherever practical.
      i) Centralized management includes the installation, configuration, management and monitoring of flaw remediation components, including:
         (1) The information systems hardware, operating system and software.
         (2) Personnel.
         (3) Automated tools.

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

For Moderate and High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs, CCPs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Use automated mechanisms on a daily basis to determine the state of information system components with regard to flaw remediation.

      Note: Organizations shall balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and with any mission or operational impacts that automatic updates might impose

      i) System flaws identified by automated tools should be automatically identified or flagged for corrective measures. Wherever possible, corrective measures shall be implemented in a controlled manner, using automated and/or manual methods, as prescribed by the SM, in coordination with the IO, ISO and IMO.
      ii) Summary flaw remediation reports shall be compiled, produced, summarized and disseminated no less than quarterly to SMs, IOs, ISOs and CSIRC. The reports shall contain the quantity and types of flaws discovered, associated components, remediation status and average time between flaw discovery and flaw resolution.

For FedRAMP Moderate and High Information Systems:

1) The SMs, in coordination with ISOs, IOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Use automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation.

SI-2 (3) – Flaw Remediation | Time to Remediate Flaws/Benchmarks for Corrective Actions

Not selected as part of the control baseline.

For FedRAMP Moderate and High Information Systems:

1) SMs, in coordination with IOs and CSIRC, for systems operated on behalf of the EPA, shall ensure service providers:

a) Use manual or automated tools to measure the time between identification of information system flaws and flaw remediation or resolution.

b) Establish time and accuracy benchmarks for flaw resolution in accordance with EPA guidance and directives.

i) Flaw remediation reports shall be produced, summarized and disseminated no less than quarterly to SMs, IOs and CSIRC. The reports shall contain the quantity and types of flaws, associated components, remediation status and average time between flaw discovery and flaw resolution.

SI-2 (4) – Flaw Remediation | Automated Patch Management Tools

Incorporated into SI-2.

SI-2 (5) – Flaw Remediation | Automatic Software/Firmware Updates

Not selected as part of the control baseline.

SI-2 (6) – Flaw Remediation | Removal of Previous Versions of Software/Firmware

Not selected as part of the control baseline.

SI-3 – Malicious Code Protection

Note: The following describes measures taken to protect against malicious code (also known as malicious software or Malware) prior to discovering that an incident has occurred. If a malicious code incident is discovered or suspected, see Appendix B: Malware Handling for the containment, isolation and eradication of Malware and recovery from Malware-related incidents. Additional information may also be found in the EPA Incident Response (IR) plan.

For All Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs, CCPs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Employ malicious code protection mechanisms at information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers), workstations,[6] servers, and mobile computing devices on the network.

b) Configure malicious code protection software to scan for malicious code automatically, at a minimum, on a daily basis.

c) Configure malicious code protection software/mechanisms to block at gateways and quarantine at host, validate quarantined code before releasing to users and clean quarantined malware as required to neutralize potential threats to the system.

i) Configure malicious code protection software to send an alert to System Administrators (SA) and the ISSO upon suspicion of malicious code and every 24 hours thereafter until the threat has been mitigated. After 72 hours, incidents shall be escalated to the ISO or/and SM. All high-risk vulnerabilities

[6] *A workstation is defined as an EPA-issued desktop, laptop, or other emerging technology.*

on Internet-accessible web applications shall be mitigated within 15 calendar days of discovery.

ii) Application-level firewalls shall be capable of and configured to detect and counter an application-level software attack and send an alert within 2 minutes of detection and blocking.

d) Direct SAs to deploy and configure malicious code protection software/mechanisms on all information systems and ensure the following:

i) Enable real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with EPA security policy.

ii) Malicious code protection software shall be updated concurrently with releases of updates provided by the vendor of the software. Updates should be tested and/or approved according to EPA requirements.

iii) Malicious code protection software shall be used to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) that is:

(1) Transported by electronic mail, electronic mail attachments, web access, removable media (e.g., Universal Serial Bus (USB) devices, diskettes, compact discs), or other means.

(2) Inserted through the exploitation of information system vulnerabilities.

(3) Encoded in various formats (e.g., UNIX-to-UNIX Encoding (UUENCODE), Unicode) or contained within a compressed file.

iv) Malicious code protection software (including signature definitions) shall be tested and updated whenever new releases are available and in accordance with agency-wide configuration management policy, procedures and standards.

(1) As applicable, the malicious code protection software/mechanisms shall be supported under a vendor SLA or maintenance contract that provides frequent updates of malicious code signatures and profiles.

(2) Refer to the latest version of the *EPA Information Security – Configuration Management Procedures* for requirements on configuration management.

v) During vendor and product selection and fine-tuning the malicious code protection software/mechanisms,[7] the following shall be addressed:

(1) False positives received during malicious code detection and eradication.

(2) Potential effects of vendor installs/updates on system/information availability.

vi) In situations where traditional malicious code protection mechanisms are not capable of detecting malicious code in software (e.g., logic bombs, back doors), the organization shall rely instead on other risk mitigation measures to include, for example, secure coding practices, code reviews, trusted procurement processes, configuration management and control and

[7] *NIST SP 800-83 and current approved anti-malware vendor guidance shall be used when implementing malicious code protection software/mechanisms.*

monitoring practices to help ensure that software does not perform functions other than those intended.

vii) System Security Plans (SSP) shall indicate the defense-in-depth strategy that integrates firewalls, routers, intrusion detection systems, antivirus software, encryption, strong authentication and cryptographic key management to ensure consistent enforcement of information security solutions and secure connections to external interfaces.

For FedRAMP Low and Moderate Information Systems:

1) SMs, in coordination with ISOs, IOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Configure malicious code protection mechanisms to:

i) Perform periodic scans of the information system at least weekly and real-time scans of files from external sources at to include endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy; and

ii) Send alert to administrator or defined security personnel in response to malicious code detection.

For FedRAMP High Information Systems:

1) SMs, in coordination with ISOs, IOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Configure malicious code protection mechanisms to:

i) Perform periodic scans of the information system at least weekly and real-time scans of files from external sources at to include endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy; and

ii) Block and quarantine malicious code and alert administrator or defined security personnel near-real time in response to malicious code detection.

<u>SI-3 (1) – Malicious Code Protection | Central Management</u>

For Moderate and High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Manage and automatically update malicious code protection software/mechanisms centrally.

i) Central management shall include server-based solutions, not client-based.

(1) The server-based solution shall automatically check for and push vendor updates to client systems.

(2) The information system shall automatically update malicious code protection software/mechanisms (including signature definitions).

<u>SI-3 (2) – Malicious Code Protection | Automatic Updates</u>

For Moderate and High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure systems to automatically update malicious code protection mechanisms, including:
      i) Vendor malicious code definition updates.
      ii) Vendor software updates.

   Note: All system software updates shall be downloaded and employed in accordance with agency-wide configuration management policy, procedures and standards.

SI-3 (3) – Malicious Code Protection | Non-Privileged Users

Incorporated into AC-6(10).

SI-3 (4) – Malicious Code Protection | Updates only by Privileged Users

Not selected as part of the control baseline.

SI-3 (5) – Malicious Code Protection | Portable Storage Devices

Incorporated into MP-7.

SI-3 (6) – Malicious Code Protection | Testing/Verification

Not selected as part of the control baseline.

SI-3 (7) – Malicious Code Protection | Non-Signature-Based Detection

Not selected as part of the control baseline.

For FedRAMP Moderate and High Information Systems:

1) SMs, in coordination with ISOs, IOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Initiate and maintain automated, non-signature based ‘heuristic’ malicious code protection mechanisms in accordance with EPA policies, procedures and standards.

SI-3 (8) – Malicious Code Protection | Detect Unauthorized Commands

Not selected as part of the control baseline.

SI-3 (9) – Malicious Code Protection | Authenticate Remote Commands

Not selected as part of the control baseline.

SI-3 (10) – Malicious Code Protection | Malicious Code Analysis

Not selected as part of the control baseline.

SI-4 – Information System Monitoring

For All Information Systems:

1) CSIRC, in coordination with the Director of OITO, SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure and monitor[8] information system hardware and software assets, to detect potential attacks, unauthorized local, network and remote connections, in accordance with the *EPA Information Security Program Plan* and *EPA Information Security Continuous Monitoring Strategic Plan*.
   b) Deploy information system monitoring devices[6] strategically within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications, with such devices typically being employed at the managed interfaces (e.g., firewalls and routers) to collect agency-determined essential information).
      i) These devices shall be used to track the impact of security changes to the information system.
      ii) Monitoring devices shall be deployed at ad hoc locations within the system to track the following:
         (1) Specific types of transactions of interest[7] to the Agency.
         (2) The impact of security changes to the information system.
      iii) The granularity of information collected shall be determined based upon agency monitoring objectives and the capability of the information system to support such activities.
   c) Collaborate with the EPA's FOIA officials, Program and Regional Officials and the Office of General Counsel or the Agency Privacy Officer to obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
   d) Heighten the level of information system monitoring activities whenever there is an indication of increased risk to EPA operations, EPA assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.
      i) The information system shall be configured to monitor inbound and outbound communications for unusual or unauthorized activities or conditions including, but not limited to:

[8] Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). 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, audit record monitoring software, network monitoring software).

[6] The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device.

[7] An example of a specific type of transaction of interest to the Agency with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required.

(1) Internal traffic that indicates the presence of malicious code within an information system or propagating among system components.

(2) The unauthorized export of information.

(3) Attack signatures.

(4) Signaling to an external information system.

(5) Localized, targeted and network-wide events.

(6) Forwarding of sensitive information via unauthorized means or via unapproved methods of transmission.

ii) Evidence of malicious code shall be used to identify potentially compromised information systems or information system components.

e) Protect the information obtained from information system monitoring tools and activities from unauthorized access, modification and deletion.

f) Configure the information system to detect and identify unauthorized wireless devices that associate or connect to the enterprise network and send a message within 10 minutes following detection to the ISSO.

i) Information systems should be configured to isolate or disconnect the specific wireless access point within one hour following detection of an unauthorized wireless device.

ii) Reconnection of wireless devices following automatic disconnect shall only be allowed following review and approval by EPA configuration management process.

g) Increase the level of monitoring activity in times of increased risk to organizational operations and assets, as directed by the SAISO, or based upon law enforcement, intelligence, or other credible sources of information.

SI-4 (1) – Information System Monitoring | Intrusion Detection System

Not Selected as part of the control baseline

For FedRAMP Moderate and High Information Systems:

1) SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Configure individual intrusion detection tools to connect to and operate within an information system-wide intrusion detection system.

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

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Employ automated tools to support near real-time analysis of events.

b) Configure automated detection tools to provide near-real time alerts regarding possible and probable intrusion events to SAs, ISOs and other essential personnel as defined within the information system’s SSP.

SI-4 (3) – Information System Monitoring | Automated Tool Integration

Not selected as part of the control baseline.

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

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure the information system to monitor inbound and outbound communications traffic for unusual activity or conditions.

For FedRAMP Moderate and High Information Systems:

1) SMs, in coordination with ISOs, IOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure the information system to continuously monitor inbound and outbound communications traffic for unusual activity or conditions.

SI-4 (5) – Information System Monitoring | System-Generated Alerts

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure the information system to provide near real-time alerts to SAs and other designated officials when indications of unusual or anomalous activity, or potential compromise occurs and is detected by the system as a result of automated reviews of the following sources:
      i) Audit records.
      ii) Input from malicious code protection mechanisms.
      iii) Intrusion detection and prevention mechanisms.
      iv) Boundary protection devices, such as firewalls, gateways and routers.

SI-4 (6) – Information System Monitoring | Restrict Non-Privileged Users

Incorporated into AC-6 (10).

SI-4 (7) – Information System Monitoring | Automated Response to Suspicious Events

Not selected as part of the control baseline.

SI-4 (8) – Information System Monitoring | Protection of Monitoring Information

Incorporated into SI-4.

SI-4 (9) – Information System Monitoring | Testing of Monitoring Tools

Not selected as part of the control baseline.

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

Not selected as part of the control baseline.

SI-4 (11) – Information System Monitoring | Analyze Communications Traffic Anomalies

Not selected as part of the control baseline.

For FedRAMP High Information Systems:

1) SMs, in coordination with ISOs, IOs, ISSOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Analyze outbound communications traffic at the external boundary of the information system and selected [Assignment: organization-defined interior points within the system (e.g. subnetworks, subsystems) to discover anomalies.

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

Not selected as part of the control baseline.

SI-4 (13) – Information System Monitoring | Analyze Traffic/Event Patterns

Not selected as part of the control baseline.

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

Not selected as part of the control baseline.

For FedRAMP Moderate and High Information Systems:

1) SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Install, connect and configure wireless intrusion detection tools strategically to create an information system-wide intrusion detection system designed to identify rogue wireless devices and detect attack attempts and potential compromises/breaches to the information system.
      i) The system shall integrate and correlate information from monitoring tools employed throughout the information system.

SI-4 (15) – Information System Monitoring | Wireless to Wireless Communications

Not selected as part of the control baseline.

SI-4 (16) – Information System Monitoring | Correlate Monitoring Information

Not selected as part of the control baseline.

For FedRAMP Moderate and High Information Systems:

1) SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Correlate the information from monitoring tools employed throughout the information system.

SI-4 (17) – Information System Monitoring | Integrated Situational Awareness

Not selected as part of the control baseline.

SI-4 (18) – Information System Monitoring | Analyze Traffic / Covert Exfiltration

Not selected as part of the control baseline.

For FedRAMP High Information Systems:

1) SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Analyze outbound communication traffic at the external boundary of the information system (i.e., system perimeter) and at (Assignment: organization-defined interior points within the system (e.g., subsystems, subnetworks)) to detect covert exfiltration of information.

SI-4 (19) – Information System Monitoring | Individuals Posing Greater Risks

Not selected as part of the control baseline.

SI-4 (20) – Information System Monitoring | Privileged User

Not selected as part of the control baseline.

SI-4 (21) – Information System Monitoring | Probationary Periods

Not selected as part of the control baseline.

SI-4 (22) – Information System Monitoring | Unauthorized Network Services

Not selected as part of the control baseline.

For FedRAMP High Information Systems:

1) SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Detect network services that have not been authorized or approved by (Assignment: organization-defined authorization or approval processes) and (Selection (one or more): audits); alerts (Assignment: organization-defined personnel or roles).

SI-4 (23) – Information System Monitoring | Host-Based Devices

Not selected as part of the control baseline.

For FedRAMP Moderate and High Information Systems

1) SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Implement host-based monitoring mechanisms which detect and counter information system attacks.

      i) Host-based monitoring mechanisms shall include a reporting element that provides reports to SAs, ISOs and other pertinent parties in cases of attack or potential attack.

SI-4 (24) – Information System Monitoring | Indicators of Compromise

Not selected as part of the control baseline.

SI-5 – Security Alerts, Advisories and Directives

For All Information Systems:

1) CSIRC, in coordination with the Director of OITO, SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Receive and disseminate information system security alerts, advisories and directives from US-CERT, vendors, developers and other designated third party alert systems on an ongoing basis.
    b) Generate, as required, internal security alerts, advisories and directives.
    c) Disseminate security alerts, advisories and directives in coordination with SOs to the SIOs, key security personnel and the EPA Patch Management Team.
        i) The EPA Patch Management Team and security personnel shall check for security alerts, advisories and directives on an ongoing basis.
    d) Obtain all security alerts, advisories and directives[8] from only reputable sources (e.g., vendors, manufacturers, government agencies, CSIRC).
    e) Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.
2) SOs, in coordination with ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Monitor and document all actions taken in response to security alerts/advisories and ensure the following are performed:
        i) Take the appropriate actions in response to security alerts/advisories[9].
            (1) Enact any updates or notices from CSIRC, per CSIRC instructions.
            (2) Contact CSIRC with any security alert/advisory concerns or questions.
            (3) Notify CSIRC when the actions are completed.
        ii) The CSIRC Coordinator shall maintain a repository of the alerts and advisories, including related communications (e.g., responses, questions, concerns) from other EPA personnel.

[8] *Security alerts and advisories are generated by US-CERT 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 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.*

[9] *The most current NIST SP 800-40 shall be used as guidance on monitoring and distributing security alerts and advisories.*

(1) Contact with special interest groups (e.g., information security forums) shall be maintained to ensure:

(a) Security-related information (e.g., threats, vulnerabilities and latest security technologies) is shared appropriately.

(b) Access is provided to advice from security professionals.

(c) Knowledge and implementation of information security best practices are current and constantly being improved.

SI-5 (1) – Security Alerts, Advisories and Directives | Automated Alerts and Advisories

For High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Employ automated mechanisms to make security alert and advisory information available throughout the organization, as needed, to ensure personnel remain aware of the latest threats.

SI-6 – Security Function Verification

For High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Configure the information system to verify the correct operation of security functions[10] when one or more of the following intervals/conditions exists:

i) At defined system transitional states (e.g., startup, restart, shutdown, abort, etc.).

ii) Upon command by a user with appropriate privilege.

iii) At least every thirty (30) calendar days.

b) Ensure the information system implements one of the following actions when anomalies are discovered:

i) Notify SA.

ii) Notify ISO.

c) Implement compensating security controls for those security functions that are not able to execute automated self-tests, or ensure the risk of not performing the verification as required is explicitly accepted.

i) The SSP shall reflect whether or not compensating security controls have been implemented or the risk has been accepted.

d) Ensure appropriate EPA information SAs and information security personnel are trained and made aware of proper procedures to shut down or restart the information system.

[10] *The need to verify security functionality applies to all security functions.*

For FedRAMP Moderate and High Information Systems

1) SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Verify that the information system checks for the correct operation of security functions upon system startup and/or restart at least monthly.
   b) Verify that the system shuts down and restarts upon command by users with appropriate privilege, or when pre-determined and configured to shut down in order to prevent damage or compromise.
   c) Verify that the system notifies the system administrator and security personnel of failed security verification tests and when anomalies are discovered.

SI-6 (1) – Security Function Verification | Notification of Failed Security Tests

Incorporated into SI-6.

SI-6 (2) – Security Function Verification | Automation Support for Distributed Testing

Not selected as part of the control baseline.

SI-6 (3) – Security Function Verification | Report Verification Results

Not selected as part of the control baseline.

SI-7 – Software, Firmware and Information Integrity

For Moderate and High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure the information systems with the automated capability to detect and identify unauthorized deviations from approved Agency baselines within 24 hours and perform hourly automated integrity checks to detect changes to the system, information, services and configuration data.
   b) Employ integrity verification applications on the information system to look for evidence of information tampering, errors and omissions.
      i) Good software engineering practices shall be employed on the information system with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and tools shall be used to monitor the integrity of the information system and the applications it hosts automatically.
      ii) The mechanism shall be able to provide a means to determine the date and time a resource was last modified or accessed depending on sensitivity.
      iii) Assessment of the integrity of software, firmware and information is performed at startup quarterly by conducting integrity scans of the information system.
   c) Document and incorporate the appropriate actions to take for the detection of unauthorized changes to software, firmware and information into the EPA incident

response capability to ensure that such events are tracked, monitored, corrected and available for historical purposes.

SI-7 (1) – Software, Firmware and Information Integrity | Integrity Checks

For Moderate and High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Employ integrity checking mechanisms designed to detect unauthorized changes to software, firmware and information to ensure that such events are tracked, monitored and corrected.
      i) The system shall perform integrity checks of software, firmware and information (e.g., evidence of tampering, errors and omissions) at startup and on an ongoing (at least quarterly) basis.

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

For High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Employ automated tools to provide notification to designated individuals upon discovering discrepancies during integrity verification.
      i) The information system shall employ automatic tools that notify the system administrators and implement logging that identifies changes when integrity violations are discovered. Fail-safe mechanisms/safeguards shall be identified in individual SSPs.

SI-7 (3) – Software, Firmware and Information Integrity | Centrally-Managed Integrity Tools

Not selected as part of the control baseline.

SI-7 (4) – Software, Firmware and Information Integrity | Tamper-Evident Packaging

Incorporated into SA-12.

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

For High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Ensure that the information system notifies the SA and ISO when integrity violations are discovered by automated integrity checking mechanisms.

SI-7 (6) – Software, Firmware and Information Integrity | Cryptographic Protection

Not selected as part of the control baseline.

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

For Moderate and High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Incorporate the detection of unauthorized operating system, software and configuration changes into the organization's incident response capability.

SI-7 (8) – Software, Firmware and Information Integrity | Auditing Capability for Significant Events

Not selected as part of the control baseline.

SI-7 (9) – Software, Firmware and Information Integrity | Verify Boot Process

Not selected as part of the control baseline.

SI-7 (10) – Software, Firmware and Information Integrity | Protection of Boot Firmware

Not selected as part of the control baseline.

SI-7 (11) – Software, Firmware and Information Integrity | Confined Environments with Limited Privileges

Not selected as part of the control baseline.

SI-7 (12) – Software, Firmware and Information Integrity | Integrity Verification

Not selected as part of the control baseline.

SI-7 (13) – Software, Firmware and Information Integrity | Code Execution in Protected Environments

Not selected as part of the control baseline.

SI-7 (14) – Software, Firmware and Information Integrity | Binary or Machine-Executable Code

For High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Prohibit the use of binary or machine executable code from sources with limited or no warranty and without the provision of source code.
        i) Exceptions to the requirement are provided only for compelling mission/operational needs and with the approval of the AO.

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

Not selected as part of the control baseline.

SI-7 (16) – Software, Firmware and Information Integrity | Time Limit on Process Execution W/O Supervision

Not selected as part of the control baseline.

SI-8 – Spam Protection

For Moderate and High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Employ spam protection mechanisms at information systems entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web access, or other common means.
   b) Enable automatic updates on spam protection mechanisms (including signature definitions) when new releases are available in accordance with the Agency's configuration management policy and procedures.[11]
      i) Spam protection mechanisms shall be configured to perform the following:
         (1) Maintain a list of authorized Internet Protocol (IP) addresses or ensure authorized sources will always be allowed.
         (2) Block a list of senders that have been verified as sending spam.
         (3) Allow users to tag or block suspected spam messages that were not detected by the spam mechanism.
      ii) EPA shall give consideration to using spam protection[12] software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).

SI-8 (1) – Spam Protection | Central Management

For Moderate and High Information Systems:

1) SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Manage connected spam protection mechanisms centrally in order to ensure comprehensive, consistent and complete spam detection, prevention and control.

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

For Moderate and High Information Systems:

1) SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

[11] Refer to Information Security – Configuration Management Procedures for requirements on configuration management.

[12] The most current version of NIST SP 800-45 shall be used as guidance on electronic mail security.

a) Ensure that information systems spam protection mechanisms are configured to update using the latest vendor updates automatically.

SI-8 (3) – Spam Protection | Continuous Learning Capability

Not selected as part of the control baseline.

SI-9 – Information Input Restrictions

Incorporated into AC-2, AC-3, AC-5 and AC-6.

SI-10 – Information Input Validation

For Moderate and High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure the information system to check the validity of the syntax and semantics of inputs.
   b) Verify the checks for input validation as part of system testing.
      i) Configure the information system to check all arguments or input data strings submitted by users, external processes, or untrusted internal processes.
   c) Configure the information system to validate all values that originate externally to the application program itself, including arguments, environment variables and information system parameters.
   d) Ensure automated data entry transmittal from other servers is in compliance with requirements set forth in the procedures found in the *EPA Information Security – Access Control Procedures*.
   e) Configure the system to send alert notifications to SAs and ISOs within 24 hours of detecting application-level software attack attempts.
   f) Configure the system to scan Internet-accessible web applications weekly, at a minimum and send alerts to SAs and ISOs.
   g) Configure the information system to send an alert within 24 hours if a scan is not completed successfully and every 24 hours afterward until a scan is completed.
      i) Escalate incidents after 72 hours of non-resolution.
   h) Mitigate all high-risk vulnerabilities within 15 calendar days of discovery.
   i) Configure the information system to trust only reliable external entities that have been identified by authorized EPA personnel.
      i) Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) shall be in place to verify that inputs match specified definitions for format and content.
   j) Configure the information system to perform the following input validations:
      i) Type checks – Checks to ensure that the input is, in fact, a valid data string and not any other type of object.

i) This includes validating that input strings contain no inserted executable content or active content that can be mistakenly interpreted as instructions to the system, including, but not limited to: Trojan horses, malicious code, metacode, metadata, or metacharacters, Hypertext Markup Language (HTML), Extensible Markup Language (XML), JavaScript, Structured Query Language (SQL) statements, shell script and streaming media.

ii) Inputs passed to interpreters shall be prescreened to prevent the content from being unintentionally interpreted as commands.

ii) Format and syntax checks – Checks to verify that data strings conform to defined formatting and syntax requirements for that type of input.

iii) Parameter and character validity checks – Checks to verify that any parameters or other characters entered, including format parameters for routines that have formatting capabilities, have recognized valid values.

i) Any parameters that have invalid values shall be rejected and discarded.

ii) Configure web server applications to prohibit invalid data from web clients in order to mitigate web application vulnerabilities including, but not limited to, buffer overflow, cross-site scripting, null byte attacks, SQL injection attacks and HTTP header manipulation.

k) Ensure invalid inputs or error statements do not give the user sensitive data, storage locations, database names, or information about the application or information system's architecture.

SI-10 (1) – Information Input Validation | Manual Override Capability

Not selected as part of the control baseline.

SI-10 (2) – Information Input Validation | Review/Resolution of Errors

Not selected as part of the control baseline.

SI-10 (3) – Information Input Validation | Predictable Behavior

Not selected as part of the control baseline.

SI-10 (4) – Information Input Validation | Timing Interactions

Not selected as part of the control baseline.

SI-10 (5) – Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats

Not selected as part of the control baseline.

SI-11 – Error Handling

For Moderate and High Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Configure the information system to generate error messages that provide information necessary for corrective actions without revealing sensitive information (e.g., account numbers, social security numbers and credit card numbers) or potentially harmful information in error logs and administrative messages that could be exploited by adversaries.

i) Error messages revealed to users shall not include file pathnames or system architecture information.

ii) Alert error messages revealed to the administrator shall include file pathnames or system architecture information and shall be written to the application's error log and audit trail.

b) Ensure information system personnel carefully consider and analyze the structure and content of error messages.

i) The criticality or severity level of error messages for the information system shall be determined.

ii) The information system is configured to reveal error messages only to authorized personnel (e.g., systems administrators, maintenance personnel).

c) Ensure the extent to which the information system is able to identify and handle error conditions is guided by operational requirements.

d) Ensure the information system's error-handling mechanisms enable the administrator to configure the application to terminate processes gracefully, when appropriate, in response to various errors and failures.

SI-12 – Information Handling and Retention

For All Information Systems:

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Handle and retain information collected or maintained by or on behalf of the Agency, including Controlled Unclassified Information (CUI),[13] within and output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards and operational requirements.

b) Ensure collaboration between EPA's FOIA officials, Program and Regional Officials, the Office of General Counsel (OGC) or other Agency representatives, as needed, to determine which information output from the information system is considered not publicly available.

c) Ensure output handling and retention requirements cover the full life cycle of the information which, in some cases, may extend beyond the disposal of the information system.

[13] *NARA designates specific information categories as CUI; consistent with the guidance, EPA shall apply appropriate controls to protect against the unauthorized dissemination of CUI. Refer to the National Archives web site: http://www.archives.gov/cui/registry/category-list.html for guidance and definition.*

d) Ensure collaboration with EPA Records Program personnel, identifying the correct records disposition for information outputs, including how to retain, transfer, archive and dispose of them.

i) Records with expired retention periods shall be disposed of in accordance with EPA guidance.

ii) When information (either electronic or printed) is no longer needed, the media shall be destroyed in accordance with the media protection procedures and standards found in Information Security – Media Protection Procedures.

iii) Record retention shall be in accordance with the guidance from the National Archives and Records Administration (NARA) and the EPA Records Management Office.

e) Prohibit auto-forwarding or auto-redirecting of EPA email outside of the EPA.gov domain.

i) An automatic forward may not be placed on an EPA mailbox to send information collected or maintained by or on behalf of the Agency to a personal or non-EPA email account. Users may manually forward individual messages that do not contain CUI, sensitive information, or other information collected or maintained by or on behalf of the Agency.

f) Ensure information system users encrypt all emails containing sensitive information using an encryption methodology approved for use by the Federal government.

g) Confirm that all personnel complete the required security awareness training[14] on the proper handling and protection of information outputs.

2) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

Configure information systems to detect, filter and block attachment downloads from personal webmail accounts.

SI-13 – Predictable Failure Prevention

Not selected as part of the control baseline.

SI-13 (1) – Predictable Failure Prevention | Transferring Component Responsibilities

Not selected as part of the control baseline.

SI-13 (2) – Predictable Failure Prevention | Time Limit On Process Execution Without Supervision

Incorporated into SI-7(16).

SI-13 (3) – Predictable Failure Prevention | Manual Transfer Between Components

[14] *Refer to the Information Security – Awareness and Training Procedures for security awareness and training requirements.*

Not selected as part of the control baseline.

SI-13 (4) – Predictable Failure Prevention | Standby Component Installation/Notification

Not selected as part of the control baseline.

SI-13 (5) – Predictable Failure Prevention | Failover Capability

Not selected as part of the control baseline.

SI-14 – Non-Persistence

Not selected as part of the control baseline.

SI-14 (1) – Non-Persistence | Refresh from Trusted Sources

Not selected as part of the control baseline.

SI-15 – Information Output Filtering

Not selected as part of the control baseline.

SI-16 - Memory Protection

For Moderate and High Information Systems

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure workstations, mobile computing devices and servers to use data execution prevention and address space layout randomization to protect memory from unauthorized code execution.
      i) Use appropriate and reasonable measures that are commensurate with the information system’s sensitivity level.

SI-17 – Fail-Safe Procedures

For Moderate and High Information Systems

1) The Director of OITO, in coordination with SOs, ISOs, IMOs, ISSOs and SMs, for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Configure the information system to alert SAs and other operator personnel within 1 hour when the following events occur:
      i) Loss of communication between critical information system components.
      ii) Loss of communication between critical components and operational facilities.
   b) Configure the system to provide specific instructions to notified personnel regarding subsequent steps to take if escalation is required to resolve the loss of communication.

7. ROLES AND RESPONSIBILITIES

Senior Agency Information Security Officer (SAISO)

1) The SAISO has the following responsibilities with respect to system and information integrity:
    a) Carry out the CIO security responsibilities under FISMA and serve as the primary liaison for the CIO to the organization's AO, SOs, CCPs and ISOs.
    b) Possess professional qualifications, including training and experience, required to administer the information security program functions and maintain information security duties as a primary responsibility.
    c) Incorporate a Patch, Vulnerability Management Plan and flaw remediation into EPA's configuration management plan and processes.

Computer Security Incident Response Capability (CSIRC)

1) CSIRC has the following responsibilities with respect to system and information integrity:
    a) Develop and implement a capability to identify, through CWE or CVE reporting sources, potential system flaws and report them to SOs, ISOs, ISSOs and others for remediation and tracking.
    b) Monitor US-CERT, NIST NVD, Vendor and Developer Sites, and other third-party alert systems.
    c) Produce notifications for vulnerabilities and remediation.
    d) Configure, wherever practical and possible, operating systems and applications for EPA information systems and mobile devices to perform automatic updates.
    e) Configure and monitor information system hardware and software assets, to detect potential attacks, unauthorized local, network and remote connections.
    f) Deploy information system monitoring devices strategically within the information system to collect agency-determined essential information.
    g) Collaborate with the EPA's FOIA officials, Program and Regional Officials and the OGC or the Agency Privacy Officer to obtain legal opinion with regard to information system monitoring activities.
    h) Heighten the level of information system monitoring activities whenever there is an indication of increased risk to EPA operations, EPA assets, individuals, other organizations, or the Nation.
    i) Protect the information obtained from information system monitoring tools and activities from unauthorized access, modification and deletion.
    j) Configure the information system to detect and identify unauthorized wireless devices that associate or connect to the enterprise network and send a message within 10 minutes following detection to the ISSO.
    k) Receive and disseminate information system security alerts, advisories and directives from US-CERT, vendors, developers and other designated third party alert systems on an ongoing basis.
    l) Generate and disseminate internal security alerts, advisories and directives.

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

n) Maintain a repository of alerts, advisories and directives, as well as responses from other EPA personnel regarding the alerts, advisories and directives, including questions and reported problems.

o) Assess and assign priority to alerts, advisories and directives for remediation actions.

p) Determine appropriate lists for distribution of alerts, advisories and directives to include at a minimum (i) the SAISO, (ii) primary and backup ISOs, (iii) ISSOs and (iv) appropriate information system management and administration personnel.

q) Oversee and develop reports on remediation actions from alerts, advisories and directives as required by the SAISO and in response to requirements of OMB and US-CERT.

r) Analyze issues associated with application of remediation actions for management resolution.

Agency Privacy Officer (APO)

1) The APO has the following responsibilities with respect to system and information integrity:

a) Assist in determining which information output from the information system is considered non-public and/or contains Privacy Act Information or Personally Identifiable Information (PII) in accordance with Privacy Procedures and Roles and Responsibilities.

Freedom of Information Act (FOIA) Officials

1) FOIA Officials have the following responsibilities with respect to system and information integrity:

a) Assist program and regional managers and staff in determining which information output from the information system is considered non-public information.

Director of Office of Information Technology Operations (OITO)

1) The Director of OITO has the following responsibilities with respect to system and information integrity:

a) Develop, document, and disseminate to all EPA employees, contractors and other users of EPA systems a system and information integrity policy and procedure.

b) Assist CSIRC, ISOs and SOs in determining threats and risks levels, in addition to setting the criteria for flaw remediation.

c) Ensure all patches, hotfixes, firmware, etc. are continuously updated, tested prior to installation and obtained from trusted vendors.

d) Ensure Agency/Industry approved tools are used to track, record and report flaw remediation and vulnerabilities.

e) Employ malicious code protection mechanisms at information system entry and exit points.

f) Configure malicious code protection software/mechanisms to scan for malicious code, block at gateways and quarantine at host, validate quarantined code before releasing to users and clean quarantined malware as required to neutralize potential threats to the system.

g) Manage and automatically update malicious code protection software/mechanisms centrally.

h) Develop a schedule for the release and implementation of patches, service packs and hot fixes for Agency-standard configurations.

i) Confirm the automated deployment of patches to IT devices using EPA authorized automated patch management tools.

j) Configure the information system to verify the correct operation of security functions.

k) Implement compensating security controls for those security functions that are not able to execute automated self-tests, or ensure the risk of not performing the verification as required is explicitly accepted.

l) Ensure appropriate EPA information SAs and information security personnel are trained and made aware of proper procedures to shut down or restart the information system.

m) Configure the information systems with the automated capability to detect and identify unauthorized deviations from approved Agency baselines within 24 hours and perform hourly automated integrity checks to detect changes to the system, information, services and configuration data.

n) Document and incorporate the appropriate actions to take for the detection of unauthorized changes to software, firmware and information into the EPA incident response capability to ensure that such events are tracked, monitored, corrected and available for historical purposes.

o) Employ integrity checking mechanisms designed to detect unauthorized changes to software, firmware and information to ensure that such events are tracked, monitored and corrected.

p) Incorporate the detection of unauthorized operating system, software and configuration changes into the organization’s incident response capability.

q) Prohibit the use of binary or machine executable code from sources with limited or no warranty and without the provision of source code.

r) Employ spam protection mechanisms at information systems entry and exit points and at workstations, servers, or mobile computing devices on the network.

s) Enable automatic updates on spam protection mechanisms when new releases are available in accordance with the Agency’s configuration management policy and procedures.

t) Configure the information system to check the validity of the syntax and semantics of inputs.

u) Configure the information system to validate all values that originate externally to the application program itself, including arguments, environment variables and information system parameters.

v) Ensure automated data entry transmittal from other servers is in compliance with requirements set forth in the procedures found in the *EPA Information Security – Access Control Procedures*.

w) Configure the system to scan Internet-accessible web applications weekly, at a minimum and send alert notifications to SAs and ISOs within 24 hours of detecting application-level software attack attempts.

x) Mitigate all high-risk vulnerabilities within 15 calendar days of discovery.

y) Configure the information system to trust only reliable external entities that have been identified by authorized EPA personnel.

z) Ensure invalid inputs or error statements do not give the user sensitive data, storage locations, database names, or information about the application or information system's architecture.

aa) Ensure information system personnel carefully consider and analyze the structure and content of error messages.

bb) Ensure the extent to which the information system is able to identify and handle error conditions is guided by operational requirements.

cc) Ensure the information system's error-handling mechanisms enable the administrator to configure the application to terminate processes gracefully, when appropriate, in response to various errors and failures.

dd) Handle and retain information collected or maintained by or on behalf of the Agency, including CUI, within and output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards and operational requirements.

ee) Ensure collaboration between EPA's FOIA officials, Program and Regional Officials, the OGC or other Agency representatives, as needed, to determine which information output from the information system is considered not publicly available.

ff) Ensure collaboration with EPA Records Program personnel, identifying the correct records disposition for information outputs, including how to retain, transfer, archive and dispose of them.

gg) Prohibit auto-forwarding or auto-redirecting of EPA email outside of the EPA.gov domain.

hh) Ensure information system users encrypt all emails containing sensitive information using an encryption methodology approved for use by the Federal government.

ii) Confirm that all personnel complete the required security awareness training on the proper handling and protection of information outputs.

jj) Configure information systems to detect, filter and block attachment downloads from personal webmail accounts

kk) Configure workstations, mobile computing devices and servers to use data execution prevention and address space layout randomization to protect memory from unauthorized code execution.

ll) Configure the system to provide specific instructions to notified personnel regarding subsequent steps to take if escalation is required to resolve the loss of communication.

System Owner (SO)

1) SOs have the following responsibilities with respect to system and information integrity:
   a) Assist with determining appropriate security measures or information system input and output and non-public information.
   b) Ensure the latest patches and versions are used and installed for current and new devices in inventory.
   c) Prioritize vulnerabilities and remediation actions based on the individual vulnerability criticality or severity ratings.
   d) Establish priorities based on the source's assessment of severity or criticality as high, moderate, or low.
   e) Modify, document and retain, as necessary, source severity assessments (other than those established by US-CERT in accordance with detailed knowledge of criteria specific to the EPA by using NVD CVSS Version 2.0 calculator provided the criteria, ratings and results are documented and retained for the record and the alteration is noted in the alert.
   f) Ensure flaw remediation and vulnerability management processes are applied to the information system
   g) Manage and report flaw remediation to the SAISO through the POA&M process via the Agency's FISMA reporting and tracking tool.
   h) Use current change management procedures for testing low priority remediation and, when possible, for testing patches and configuration modifications of moderate priority vulnerabilities.
   i) Obtain approval or request a waiver through the CIO for non-standard IT products for use within the Agency and shall ensure the non-standard products are tested using approved configuration standards.
   i) Guarantee that when automated tools are not feasible, installation shall be verified by manual methods and supported with documented evidence.
   j) Report to CSIRC via the Agency incident reporting system and provide necessary evidence upon request, unless the status is available through an automated tool visible to CSIRC personnel.
   k) Verify the completion of procedures contained in US-CERT guidance and Information Assurance Vulnerability Alerts.
   l) Procure and oversee the deployment of malicious code protection software to support the near real-time analysis of events.
   m) Configure the information system to monitor inbound and outbound communications traffic for unusual activity or conditions.
   n) Configure the information system to provide near real-time alerts to SAs and other designated officials when indications of unusual or anomalous activity, or potential compromise occurs and is detected by the system as a result of automated reviews.
   o) Monitor and document all actions taken in response to security alerts/advisories. Ensure the extent to which the information

p) Develop and maintain the security plan and ensure that the information system is deployed and operated

Information Security Officers (ISO)

1) ISOs have the following responsibilities with respect to system and information integrity:
   a) Assist the SO in carrying out their responsibilities as needed.
   b) Maintain an inventory of all components of their information system.
   c) Monitor and check for security alerts, advisories and directives on an ongoing basis for all non-standard components of their information system.
   d) Ensure appropriate prioritization of remediation for standard and non-standard IT resources.
   e) Respond to alerts, advisories and directives related to components of the information systems by taking appropriate remediation actions within established time frames.
   f) Report any issues associated with application of remediation actions to CSIRC.
   g) Assign individuals to test remediation of information system components.
   h) Train individuals assigned to test information system components as needed.
   i) Maintain distribution lists for alerts, advisories and directives.
   j) Distribute alerts, advisories and directives to information system users as appropriate or requested.

Information System Security Officer (ISSO)

1) ISSOs have the following responsibilities with respect to system and information integrity:
   a) Assist SOs, IOs and IMOs in carrying out their responsibilities.
   b) Assist in verifying that remediation actions have been successfully implemented.

Service Managers (SM)

1) SMs have the following responsibilities with respect to system and information integrity:
   a) Review and update the current system and information integrity policy and procedures.
   b) Install security-relevant software and firmware updates.
   c) Use automated mechanisms to determine the state of information system components with regard to flaw remediation.
   d) Use manual or automated tools to measure the time between identification of information system flaws and flaw remediation or resolution.

e) Establish time and accuracy benchmarks for flaw resolution in accordance with EPA guidance and directives.

f) Configure malicious code protection mechanisms to perform periodic scans of the information system and real-time scans of files from external sources to include endpoints.

g) Send alert to administrator or defined security personnel in response to malicious code detection.

h) Configure individual intrusion detection tools to connect to and operate within an information system-wide intrusion detection system.

i) Configure the information system to continuously monitor inbound and outbound communications traffic for unusual activity or conditions.

j) Analyze outbound communications traffic at the external boundary of the information system to discover anomalies.

k) Install, connect and configure wireless intrusion detection tools strategically to create an information system-wide intrusion detection system designed to identify rogue wireless devices and detect attack attempts and potential compromises/breaches to the information system

l) Correlate the information from monitoring tools employed throughout the information system.

m) Implement host-based monitoring mechanisms which detect and counter information system attacks

n) Verify that the information system checks for the correct operation of security functions upon system startup and/or restart at least monthly.

o) Verify that the system shuts down and restarts upon command by users with appropriate privilege, or when pre-determined and configured to shut down in order to prevent damage or compromise.

p) Verify that the system notifies the system administrator and security personnel of failed security verification tests and when anomalies are discovered.

Information Owners (IO)

1) IOs have the following responsibilities with respect to system and information integrity:

   a) Assist SO, ISO and OITO with ensuring flaw remediation and patch and vulnerabilities management procedures are implemented appropriately.

   b) Assist in verifying that remediation actions have been successfully implemented.

   c) Assist with ensuring the information system input/output, error messages and integrity checks are configured and operate as intended.

Common Control Provider (CCP)

1) CCPs have the following responsibilities with respect to system and information integrity:

a) Assist the SO, IMO, ISSO, IO and SMs with implementing, assessing, configuring, monitoring and maintaining common controls to adequately protect information systems.

b) Assist SO with flaw remediation actions for discovered weaknesses based on risk decisions. Document risk decisions regarding discovered weaknesses to include transfer and acceptance.

8. RELATED INFORMATION

- NIST Special Publications, 800 series
- Related policy and procedures are available on OEI's Policy Resources Intranet site: http://intranet.epa.gov/oei/imitpolicy/policies.htm
- Related standards and guidelines are available on OEI's website.

9. 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.
- **Information Type**: a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
- **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.
- **Privacy Act Information**: data about an individual that is retrieved by name or other 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**: the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- **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.
- **Written** (or in writing): means to officially document the action or decision, either manually or electronically and including a signature.

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- substantive business case need(s)
- demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the Agency.

The SAISO and Director of OITO shall coordinate to maintain a central repository of all waivers.

11. MATERIAL SUPERSEDED

- EPA Information Procedure: CIO 2150-P-17.1, Interim Information Security – System and Information Security Procedures, July 18, 2012.

12. CONTACTS

For further information, please contact the Office of Environmental Information (OEI), Office of Information Security and Privacy (OISP).

Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A:
Acronyms & Abbreviations

AO	Authorizing Official
APO	Agency Privacy Officer
BIOS	Basic Input/Output System
CCP	Common Control Provider
CIO	Chief Information Officer
COTS	Commercial-Off-the-Shelf
CSIRC	Computer Security Incident Response Capability
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
GOTS	Government-Off-the-Shelf
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol - Secure
IMO	Information Management Officer
IO	Information Owner
IP	Internet Protocol
IR	Incident Response
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
LSI	Large-Scale Integration
MD5	Message Digest Algorithm 5
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OGC	Office of General Counsel
OIG	Office of Inspector General
OISP	Office of Information Security and Privacy
OITO	Office of Information Technology Operations
OMB	Office of Management and Budget
PAO	Privacy Act Officer
PGP	Pretty Good Privacy
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
SAISO	Senior Agency Information Security Officer
SCA	Security Control Assessor
SCAP	Security Content Automation Protocol
SHA-2	Secure Hash Algorithm-2
SLA	Service Level Agreement

SM	Service Manager
SO	System Owner
SP	Special Publication
SPII	Sensitive Personally Identifiable Information
SSP	System Security Plan
SQL	Structured Query Language
TLS	Transport Layer Security
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
USC	United States Code
UUENCODE	UNIX-to-UNIX Encoding
XML	Extensible Markup Language

APPENDIX B: Malware Handling

Note: This appendix is excerpted from the *EPA Information Security – Incident Response (IR) Procedure*. For more information regarding IR, IR roles and responsibilities and IR reporting, consult the EPA Incident Response plan.

[Containment and Isolation Actions]

For All Information Systems:

1) The SAISO, in coordination with SOs and IOs for EPA-operated systems; and IOs, in coordination with SMs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Institute measures to stop and contain the spread of malware and/or isolate affected systems.
   b) Enact pre-established controls to ensure priority handling of suspicious system events.
   c) Provide clear instructions to users regarding the containment of malware known to exist on the network following detection of the malware within organizational systems.
   d) Enact an organizational incident handling capability for malware-related security incidents that incorporates clear steps for incident preparation, detection, analysis, containment, eradication and recovery.
   e) Provide a process to coordinate incident handling activities and incorporate lessons-learned from past incidents, training and test/exercises.
   f) Eliminate or disable services that may be used by the malware as a means to propagate throughout the system or a network of systems and provide clear user instructions to prevent system administrators or users from performing actions that may inadvertently propagate malware across systems and networks.
   g) Offer specialized training to personnel designated to handle malware incidents and institute measures that facilitate and promote effective malware response, containment and resolution, such as:
      i) Providing malware incident trained and response-capable personnel that are available during normal business hours and on call during the off-hours.
      ii) Creating and maintaining a SLA for agency response to advisories that are received from external organizations (e.g., CERT) that may have an impact on Agency information systems.
      iii) Promoting awareness of information security risks so the Agency is better prepared to handle those incidents and is better protected against them.
      iv) Responding to malware incidents according to pre-defined response requirements.
      v) Coordinating with OITO security staff as needed for logistical support.
      vi) Developing, maintaining and publishing operational procedures required for ISO/ISSO site-specific handling of malware incidents.
      vii) Receiving and forwarding malware and vulnerability notifications to appropriate IOs, SOs and ISSOs for affected systems.

viii) Maintaining a contact list of system administrators, system managers and ISOs to enable notification and coordination according to response requirements.

ix) Establishing and maintaining notification and escalation procedures for malware incidents at the location of the information system, according to defined response requirements.

x) Using the following NIST SPs for guidance for malware and malware incident handling: 800-36, *Guide to Selecting Information Technology Security Products*; 800-61*, Computer Security Incident Handling Guide*, Revision 2; 800-83, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, Revision 1; 800-86, *Guide to Integrating Forensic Techniques into Incident Response*; 800-92, *Guide to Computer Security Log Management*; 800-94, DRAFT *Guide to Intrusion Detection and Prevention Systems* (IDPS), Revision 1; and 800- 101, *Guidelines on Mobile Device Forensics*, Revision 1.

xi) Monitoring and inventorying system locations, movement, connection status and applications prior to and during an incident in order to aid the organization of malware response activities during a malware incident.

[Eradication and Recovery Actions]

For All Information Systems:

1) The SAISO, in coordination with SOs and IOs, for EPA-operated systems; and IOs, in coordination with SMs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Use automated eradication tools such as antivirus software, specialized malware removal utilities, patch management software and root-level inspection programs as necessary to eliminate malware infections from systems and networks.

b) Repair or rebuild infected hosts to guard against the spread or reinitiating of infections.

c) Track and document all actions performed to contain or eliminate malware.

d) Maintain Malware records at the designated official repository and at the site of the incident where on-site response teams report and take incident-related actions

e) Logs shall be maintained in accordance with *EPA Records Schedule 130*.

i) Logs pertaining to a law enforcement action may subject them to retention requirements that are in accordance with *EPA Records Schedule 698*.

f) Use EPA's Remedy system (or equivalent) as the Agency repository for tracking incidents reported through the EPA Call Center (EPA CC).

i) The security incident component shall be separate from other tracking data to ensure only authorized personnel have access to the security incident information.

g) Use workflow capabilities of EPA's Remedy system (or equivalent) to request incident response assistance of the ISOs and ISSOs to respond to those requests.

h) Provide access to the Agency's incident tracking database(s) for the Office of Inspector General (OIG)-OI to aid potential criminal investigative actions.

i) Employ automated mechanisms to assist tracking of malware incidents and collecting and analyzing information regarding security incidents.

j) Report all known or suspected information security incidents or vulnerabilities immediately using the notification instructions located in IR-6, above. Once incident information is reported to CSIRC, the following actions shall be taken:

   i) CSIRC shall conduct an initial inquiry to verify whether an incident actually occurred and provide immediate mitigation, if possible.

   ii) CSIRC shall record incident information in a tracking system.

   iii) Once an incident is validated, CSIRC shall determine the magnitude of the incident, determine who to notify and, in coordination with the SAISO, immediately escalate possible crime-related events to the OIG-OI.

   iv) CSIRC shall coordinate informing other system personnel about an incident possibly affecting them, in accordance with response actions and escalation protocols established for incidents.

   v) A CSIRC Coordinator collects and disseminates incident information by:

      (1) Interfacing with the ISOs, ISSOs and US-CERT.

      (2) Reporting incidents to US-CERT, the OIG, Office of Public Affairs, the EPA Physical Security Officer and EPA Senior Management, as appropriate.