
EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

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

INFORMATION SECURITY –
INTERIM SYSTEM AND INFORMATION INTEGRITY PROCEDURES
V2.1
JULY 16, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the System and Information Integrity control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*.

2. SCOPE AND APPLICABILITY

These 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 agency.

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

3. AUDIENCE

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

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that 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 must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*. This chapter addresses the procedures and standards set forth by EPA, and in compliance with, the system and information integrity family of controls found in NIST SP 800-53, Revision 3.

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III, *Federal Information Security Management Act (FISMA)* as amended
 - 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 USC 3501-3519)
 - Privacy Act of 1974 (5 USC § 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-00-07, “*Incorporating and Funding Security in Information Systems Investments*”, February 2000
 - 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-11, “*Preparation, Submission and Execution of the Budget*”, June 2006
 - OMB Circular A-130, “*Management of Federal Information Resources*”, Appendix III, “*Security of Federal Automated Information Resources*”, November 2000
 - 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 CFR Chapter XII, Subchapter B - *Records Management* (Parts 1220-1238)
 - EPA Information Security Program Plan
 - EPA Information Security Policy
-

6. PROCEDURES

SI-2 – Flaw Remediation

- a. EPA shall identify, report, and correct information system flaws.

Note: 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.

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- b. An inventory of information systems and components must be collected and maintained in order to determine which hardware equipment, operating systems, and software applications are in operation.
- The inventory, both for the enterprise and at each office and region, must include both standard information systems and components and those not designated as agency standards (i.e., non-standard equipment, operating systems, software applications).
 - All software monitored, including the vendor, version, and support contract information, must be part of the inventory. Software types include:
 - Firmware
 - Commercial-Off-the-Shelf (COTS)
 - Government-Off-the-Shelf (GOTS)
 - Operating System, to include computer and network operating systems
 - Standard applications
 - Custom applications
- c. Flaw remediation must be incorporated into EPA's configuration management process.
- Refer to *Information Security – Configuration Management Procedures* for requirements on configuration management.
- d. A Patch and Vulnerability Management Plan must be developed as part of the Configuration Management Plan and must address the following:
- All equipment, operating systems, and software applications must be included.
 - The criteria for implementing flaw remediations must be defined with respect to:
 - Threat level
 - Risk of compromise
 - Consequences of compromise
 - The responsible party for monitoring and coordinating with each vendor for patch release support must be designated.
 - The responsible party for testing patches must be identified and coordinated.
 - Information security patches shall be installed in accordance with configuration management plans.
- e. Security sources for vulnerability announcements (i.e., both patch and non-patch remediation) and emerging threats that correspond to the software within the information system's inventory must be monitored.
- The following sources must be monitored by subscription or on a daily basis where subscription is not available:
 - United States Computer Emergency Readiness Team (US-CERT)
National Cyber Alert System
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- Vendor and developer sites
- Other third-party alert systems
- ii. When new devices are added to the inventory, the following sites must be accessed to ensure that the latest patches and versions are currently used and installed:
 - US-CERT National Cyber Alert System
 - NIST National Vulnerability Database (NVD)
 - Vendor and developer sites
 - Other third-party sites
- f. Information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) must be reported to designated organizational officials with information security responsibilities (e.g., Senior Information Security Officers, Information System Security Managers, Information Systems Security Officers).
- g. Vulnerability and remediation information must be disseminated to local system administrators and security personnel.
 - i. Standard email distribution lists must be established.
- h. System administrators must be instructed or trained on how to apply vulnerability and configuration management remediations.
 - i. Notifications of vulnerabilities and remediations must contain instructions on how to apply them, if automated mechanisms are not used.
 - ii. In special and rare circumstances, “just-in-time” training must be used, as necessary.

Note: Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems.

- i. Vulnerabilities and remediation actions must be prioritized, and their priority order must be based on the individual vulnerability criticality or severity ratings.
 - i. Priorities must be established based on the source’s assessment of severity or criticality as high, moderate/medium, or low.
 - ii. US-CERT’s established criticality takes priority.
 - iii. The next highest priority available from the following sources must be used unless EPA has established a different priority based on the application of NIST’s Common Vulnerability Scoring System (CVSS) Calculator:
 - Vendor web sites and mailing lists
 - Third-party web sites
 - Vulnerability scanner
 - Vulnerability databases
 - Enterprise patch management tools
 - Other notification tools
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- iv. Source severity assessments other than those established by US-CERT may be modified in accordance with detailed knowledge of criteria specific to the Agency, by using NIST's CVSS Calculator, provided the criteria, ratings, and results are documented and retained for the record and the alteration is noted in the alert.
 - v. NIST's CVSS Calculator must be used to establish priority as follows:
 - Vulnerabilities must be labeled "Low" severity if they have a CVSS base score of 0.0–3.9.
 - Vulnerabilities must be labeled "Medium" severity if they have a base CVSS score of 4.0–6.9.
 - Vulnerabilities must be labeled "High" or "Critical" severity if they have a CVSS base score of 7.0–10.0.
 - j. A database of remediations that need to be applied to the organization's IT resources must be created and maintained.
 - i. Vulnerability remediation must be monitored.
 - k. Software updates related to flaw remediation, (including patches, services packs, and hot fixes) must be tested before installation for effectiveness and potential side effects on EPA information systems.
 - i. The level and timing of testing may vary and depend on risk to the information system and priority of the remediation.
 - Fixes for vulnerabilities ranked high or critical must be tested as soon as possible but no later than two business days.
 - Fixes for vulnerabilities ranked moderate or medium must be tested within seven business days.
 - Complete testing of fixes for low priority vulnerabilities must be completed within 30 days.
 - ii. Existing change management procedures must be used for testing low priority remediations and, when possible, for testing patches and configuration modifications of moderate/medium priority vulnerabilities.
 - i. The flaw remediation process must be centrally managed and software updates must be installed automatically.
 - ii. The software code for all patches, service packs, hot fixes, etc., must be verified before testing or installation.
 - A vendor authentication mechanism (e.g., cryptographic checksums, Pretty Good Privacy [PGP] signatures, digital certificates) must be used to ensure the authenticity of the code.
 - a. SHA-1 checksums from vendors must be used, instead of MD5 or similar checksums, whenever they are available.
 - The code must be scanned for viruses using the most current virus signature database.
 - A search must be performed to learn what experiences others have had in installing or using the patch.
 - iii. All remediation changes must be tested on non-production systems prior to
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

implementation on all agency-standard IT products and configurations in order to reduce or eliminate the following:

- Unintended consequences
 - Alteration of security settings
 - Enabling of default user accounts that had been disabled
 - Resetting of default passwords for user accounts
 - Enabling of services and functions that had been disabled
 - Non-security changes, such as new functionality
- iv. Testing of patches must ensure that patches are installed in the required sequence and any removal of any previous security patch is not unintended.
 - v. Testing must include checking all related software to ensure that it is operating correctly.
 - vi. Testing must include a selection of systems that accurately represent the configuration of the systems in deployment.
 - Testing of remediations must be conducted on IT components that use standardized configurations.
 - Images of standard configurations must be used on test systems or within virtual machines on test systems that can expedite the testing process.
 - Non-standard IT products that have been approved for use within the Agency must be tested using approved configurations.
 - b. Based on the results of testing, it must be considered whether any significant disadvantages outweigh the benefits of installing a patch and whether remediation should be delayed.
 - i. If the potential negative consequences are significant, then the following must be considered:
 - Waiting until the vendor releases a newer patch that corrects the major issues
 - The ability to “undo” or uninstall a patch

Note: Even when the “undo” option is provided, the uninstall process does not always return the system to its previous state, which requires a documented fix.

- ii. Delay of high or moderate/medium priority remediation must be approved by the Senior Agency Information Security Officer, (SAISO) with appropriate documentation of rationale and mitigation measures.
 - c. A schedule for the release and implementation of patches, service packs, and hot fixes for Agency-standard configurations must be developed by the SAISO, as needed, in coordination with CSIRC, and individual system security personnel.
 - i. The patch release schedule must be developed using a risk-based decision that is in compliance with pre-defined criteria (i.e., threat level, risk of compromise, and consequences of compromise) outlined in the Flaw and Vulnerability Management Plan.
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- d. Security-relevant software updates (e.g., patches, service packs, and hot fixes) must be installed promptly by EPA and any EPA contractors.
 - i. The requirements for testing and consideration of significant negative consequences of the remediation must still apply.
 - ii. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.
 - iii. The priority of the vulnerability must determine how promptly the remediation is implemented.
 - Vulnerabilities ranked high or critical must be mitigated and reported to CSIRC within two business days after testing is completed.
 - Vulnerabilities ranked moderate/medium must be mitigated and reported to CSIRC within seven business days after testing is completed.
 - Vulnerabilities ranked low must be mitigated within 30 days.
 - iv. Automated deployment of patches to IT devices using enterprise patch management tools must be performed.
 - EPA's standard tools for automated patch deployment and installation must be used.
 - When automated mechanisms are not available, feasible, or appropriate, manual patch installation and remediation must be performed.
 - v. Automated tools acquired to support vulnerability and configuration management remediation actions must be selected based on the following order of priority:
 - Tools that implement, support, and are validated by NIST to conform to the Security Content Automation Protocol (SCAP)
 - Tools that are pursuing or have a corporate commitment to conformance with NIST validation of SCAP
 - Tools that readily integrate with other SCAP-validated tools
 - Commercial tools that lack SCAP validation, in the absence of validated tools
 - Tools developed in house that readily integrate with SCAP-validated tools
 - e. Vulnerability and flaw remediation actions must be tracked and verified.
 - i. Appropriate automated tools and methods include, but are not limited to, the following:
 - Patch deployment tool database
 - Network and host vulnerability scanning
 - Configuration management tool
 - ii. Where automated tools are not feasible, installation must be verified by manual methods, including, but not limited to the following:
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- Inspecting the configuration by, for example, viewing Basic Input/Output System (BIOS) boot screen, “Help – About” or other available and appropriate verification mechanism for the hardware, operating system, or application
- 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
 - a. This may or may not be a function of the tool used.
- Reviewing patch logs
- iii. Verification must not employ exploit procedures (e.g., a penetration test) or code to exploit any vulnerabilities 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.
- iv. The accomplishment of procedures contained in US-CERT guidance and Information Assurance Vulnerability Alerts must be verified.
- f. When flaw remediation and vulnerability mitigation activities are completed, the following actions must occur:
 - i. The inventory of information systems and components must be updated to reflect current software versions and configurations.
 - ii. Stakeholders, including but not limited to EPA’s Computer Security Incident Response Capability (CSIRC), must be notified.
- g. Reporting to CSIRC must be via the Agency incident reporting system, unless status is available through an automated tool visible to CSIRC personnel.
- h. NIST SP 800-40, Version 2.0 must be used as guidance on security patch installation and patch management.

For moderate and high information systems

- i. Automated mechanisms must be able to determine the state of information system components with regard to flaw remediation daily.

For high information systems

- j. The flaw remediation process must be centrally managed and software updates must be installed automatically.
 - i. The methodology used to carry out automatic updates must be carefully considered due to information system integrity and availability concerns.

SI-3 – Malicious Code Protection

- a. Malicious code protection mechanisms must be employed at information system 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.
 - b. Configures malicious code protection mechanisms to block at gateways and quarantine at host, validate quarantined code before releasing to user, clean
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

quarantined malware as appropriate.

- c. Standard malicious code protection software deployed on all workstations and servers must be configured to adhere to the following:
 - i. Servers must be scanned for malicious code on a continuous basis.
 - ii. Workstations must be automatically scanned for malicious code on a daily basis.
 - iii. Malicious code protection software must allow users to manually perform scans on their workstation and removable media.
 - iv. Malicious code protection software must 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.
- d. Malicious code protection mechanisms must be used to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) that is:
 - i. Transported by electronic mail, electronic mail attachments, web accesses, removable media (e.g., Universal Serial Bus [USB] devices, diskettes or compact disks), or other common means
 - ii. Inserted through the exploitation of information system vulnerabilities
 - iii. Encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file
- e. Malicious code protection mechanisms (including signature definitions) must be updated whenever new releases are available and in accordance with agency-wide configuration management policy, procedures, and standards.
 - i. As applicable, the malicious code protection software must be supported under a vendor Service Level Agreement (SLA) or maintenance contract that provides frequent updates of malicious code signatures and profiles.
 - ii. Refer to *Information Security – Configuration Management Procedures* for requirements on configuration management.
- f. Malicious code protection mechanisms must be configured to:
 - i. Perform periodic scans of the information system daily and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with EPA security policy
 - ii. Block and quarantine malicious code and send alert to an administrator in response to malicious code detection
- g. The following elements must be addressed during vendor and product selection and when tuning the malicious code protection software:
 - i. The receipt of false positives during malicious code detection and eradication
 - ii. The resulting potential impact on the availability of the information

Note: A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions and business functions.

- h. 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 must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended.
- i. NIST SP 800-83 and current anti-malware vendor guidance must be used as guidance when implementing malicious code protection.
- j. SSPs shall adopt a defense-in-depth strategy that integrates firewalls, screening, routers, wireless intrusion detection systems, antivirus software, encryption, strong authentication, and cryptographic key management to ensure information security solutions and secure connections to external interfaces are consistently enforced.

For moderate and high information systems

- k. Malicious code protection mechanisms must be centrally managed.
 - i. Central management must include server-based solutions, not client-based.
 - The server-based solution must automatically check for and push out updates.
- l. The information system must automatically update malicious code protection mechanisms (including signature definitions).
- m. The information system must be configured to prevent non-privileged users from circumventing malicious code protection capabilities.

SI-4 – Information System Monitoring

For moderate and high information systems

- a. Events on the information systems must be monitored in accordance with defined monitoring objectives and information system attacks must be detected.

Note: 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).

- b. Unauthorized use of the system must be identified.
 - c. Monitors events on the information system in accordance with Agency Information Security Program Plan.
 - d. Monitoring devices must be strategically deployed within the information system
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

(e.g., at selected perimeter locations, near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17) to collect agency-determined essential information.

- i. These devices must be used to track the impact of security changes to the information system.

Note: The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device.

- e. Monitoring devices must be deployed at ad hoc locations within the system to track the following:
 - i. Specific types of transactions of interest to the Agency
 - ii. The impact of security changes to the information system

Note: 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.

- f. The granularity of information collected must be determined based upon agency monitoring objectives and the capability of the information system to support such activities.
 - g. EPA shall obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
 - h. EPA shall heighten the level of information system monitoring activity 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 must be configured to monitor inbound and outbound communications for unusual or unauthorized activities or conditions including, but not limited to:
 - i. Internal traffic that indicates the presence of malicious code within an information system or propagating among system components
 - ii. The unauthorized export of information
 - iii. Attack signatures
 - iv. Signaling to an external information system
 - v. Localized, targeted, and network-wide events
 - j. Evidence of malicious code must be used to identify potentially compromised information systems or information system components.
 - k. Automated tools must be employed to support near real-time analysis of events.
 - l. The information system must be configured to provide a near real-time alert when indications of compromise or potential compromise occur from the following sources:
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- 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
- m. The information system must be configured to prevent non-privileged users from circumventing intrusion detection and prevention capabilities.
- n. NIST SP 800-61, Revision 1 must be used as guidance on responding to attacks through various types of security technologies.
- o. NIST SP 800-83 must be used as guidance on responding to detecting malware-based attacks.
- p. NIST SP 800-92 must be used as guidance on monitoring and analyzing computer security event logs.
- q. NIST SP 800-94 must be used as guidance on intrusion detection and prevention.

SI-5 – Security Alerts, Advisories, and Directives

- a. EPA shall receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis.
- b. Internal security alerts, advisories, and directives must be generated, as deemed necessary.
- c. Security alerts, advisories, and directives must be disseminated to EPA personnel
 - i. Information system and security personnel shall check for security alerts, advisories, and directives on an ongoing basis.
 - All security alerts, advisories, and directives must be from reputable sources (i.e., vendors, manufacturers, government agencies, CSIRC).
- d. Security directives must be implemented in accordance with established time frames, or the issuing organization must be notified of the degree of noncompliance.

Note: 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 affects on organizational operations and assets, individuals, other organizations, and the nation should the directives not be implemented in a timely manner.

- e. The types of actions to be taken in response to security alerts/advisories must be documented.
 - f. Information system personnel shall take appropriate actions in response to security alerts/advisories.
 - i. Any updates or notices from CSIRC must be implemented per CSIRC instructions.
 - ii. CSIRC must be contacted with any security alert/advisory concerns or
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

questions.

- iii. CSIRC must be notified when the actions are completed.
- g. The coordinator for CSIRC shall maintain a repository of the alerts and advisories, including related communications (i.e., responses, questions, concerns) from other EPA personnel.
- h. EPA shall maintain contact with special interest groups (e.g., information security forums) that:
 - i. Facilitate sharing of security-related information (eg, threats, vulnerabilities, and latest security technologies)
 - ii. Provide access to advice from security professionals
 - iii. Improve knowledge of security best practices
- i. NIST SP 800-40, Version 2.0 must be used as guidance on monitoring and distributing security alerts and advisories.

For high information systems

- j. EPA shall employ automated mechanisms to make security alert and advisory information available throughout the organization as needed.

SI-6 – Security Functionality Verification

For high information systems

- a. The information system must verify the correct operation of security functions at one of the following intervals:
 - i. At defined system transitional states (eg, startup, restart, shutdown, abort)
 - ii. Upon command by a user with appropriate privilege
 - iii. At least every 30 days
- b. The information system must implement one of the following actions when anomalies are discovered:
 - i. Notify system administrator.
 - ii. Notify ISO,

Note: The need to verify security functionality applies to all security functions.

- c. For those security functions that are not able to execute automated self-tests, compensating security controls must be implemented or the risk of not performing the verification as required must be explicitly accepted.
 - i. The System Security Plan must reflect whether or not compensating security controls have been implemented or the risk has been accepted.
- d. The appropriate EPA personnel must be trained and made aware of proper procedures to shut down or restart the information system.

SI-7 – Software and Information Integrity

For moderate and high information systems

- a. The information system must be configured to detect unauthorized changes to

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

software and information.

- b. Integrity verification applications must be employed on the information system to look for evidence of information tampering, errors, and omissions.
- c. Good software engineering practices must 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 must be used to automatically monitor the integrity of the information system and the applications it hosts.
 - i. The mechanism should be able to provide a means to determine the date and time a resource was last modified or accessed depending on sensitivity.
- d. EPA shall reassess the integrity of software and information by performing quarterly integrity scans of the information system.

For high information systems

- e. Automated tools must be employed that provide notification to designated individuals upon discovering discrepancies during integrity verification.

SI-8 – Spam Protection

For moderate and high information systems

- a. Spam protection mechanisms must be employed 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.
 - b. Centrally manages spam protection mechanisms.
 - c. Spam protection mechanisms must be used to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means.
 - d. Spam protection mechanisms (including signature definitions) must be updated when new releases are available.
 - i. Updates are implemented in accordance with EPA configuration management policy and procedures.
 - Refer to *Information Security – Configuration Management Procedures* for requirements on configuration management.
 - e. Spam protection mechanisms must be configured to perform the following:
 - i. Maintain a list of authorized Internet Protocol (IP) addresses or ensure authorized sources will always be allowed.
 - ii. Block a list of senders that have been verified as sending spam.
 - iii. Allow users to tag or block suspected spam messages that were not detected by the spam mechanism.
 - f. EPA shall give consideration to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).
 - g. NIST SP 800-45, Version 2, must be used as guidance on electronic mail security.
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

For high information systems

- h. Spam protection mechanisms must be centrally managed.

SI-9 – Information Input Restrictions

For moderate and high information systems

- a. The capability to input information to the information system must be restricted to authorized personnel.

Note: Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

SI-10 – Information Input Validation

For moderate and high information systems

- a. The information system must be configured to check the validity of information inputs.
 - i. The checks for input validation must be verified as part of system testing.
 - b. The information system must be configured to check all arguments or input data strings submitted by users, external processes, or untrusted internal processes.
 - i. The information system must validate all values that originate externally to the application program itself, including arguments, environment variables, and information system parameters.
 - ii. Automated data entry transmittal from other servers must comply with requirements set forth in the procedures found in *Information Security – Access Control Procedures*.
 - iii. The information system must trust only reliable external entities which have been identified by authorized EPA personnel.
 - c. Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) must be in place to verify that inputs match specified definitions for format and content.
 - d. The information system must be configured 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.
 - 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.
 - Inputs passed to interpreters must 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
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

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.
 - Any parameters that have invalid values must be rejected and discarded.
 - Web server applications must be configured 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.
- e. Invalid inputs or error statements must not give the user sensitive data, storage locations, database names, or information about the application or information system's architecture.

SI-11 – Error Handling

For moderate and high information systems

- a. The information system must be configured to identify potentially security-relevant error conditions.
- b. The structure and content of error messages must be carefully considered by information system personnel.
 - i. The criticality or severity level of error messages for the information system must be determined.
- c. The information system must be configured to reveal error messages only authorized personnel.
 - i. System error messages must be revealed only to authorized personnel (e.g., systems administrators, maintenance personnel).
- d. Error messages generated by the information system must provide information necessary for corrective actions without revealing sensitive information (e.g., account numbers, social security numbers, 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 must not include file pathnames or system architecture information.
 - ii. Alert error messages revealed to the administrator must include file pathnames or system architecture information and must be written to the application's error log and audit trail.
- e. The extent to which the information system is able to identify and handle error conditions must be guided by operational requirements.
- f. The information system's error-handling mechanisms must enable the administrator to configure the application to gracefully terminate processes, when appropriate in response to various errors and failures.

SI-12 – Output Handling and Retention

- a. Both information within and output from the information system must be handled
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

and retained in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

- i. EPA's FOIA officials, in consultation with program officials, the Office of General Counsel or the Privacy Act Officer, as needed, shall determine which information output from the information system is considered not publicly available.
 - ii. Output handling and retention requirements must cover the full life cycle of the information, which in some cases, may extend beyond the disposal of the information system.
 - iii. EPA Records Program shall identify the correct records disposition for information outputs, including how to retain, transfer, archive, and dispose of them.
 - Records with expired retention periods must be disposed of in accordance with EPA guidance.
 - When information (either electronic or printed) no longer becomes necessary, the media must be destroyed in accordance with the media protection procedures and standards found in Information Security – Media Protection Procedures.
 - Record retention must be in accordance with the guidance from the National Archives and Records Administration (NARA).
 - iv. Auto-forwarding or redirecting of EPA email outside of the .gov domain is prohibited and shall not be used. An automatic forward may not be placed on an EPA mailbox to send to a personal or non-EPA business email account. Users may manually forward individual messages after determining that the risk or consequences are low.
 - When sending email to an address outside of the .gov domain, users shall ensure that any sensitive information, particularly PII, is appropriately protected, i.e., encrypted.
 - b. EPA shall ensure that all personnel receive security awareness training on the proper handling and protection of information outputs.
 - i. Refer to *Information Security – Awareness and Training Procedures* for requirements on security awareness training.
-

7. RELATED DOCUMENTS

- NIST SP 800-40, Version 2.0, *Creating a Patch and Vulnerability Management Program*, November 2005
 - NIST SP 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007
 - NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009
 - NIST SP 800-61, Revision 1, *Computer Security Incident Handling Guide*, March 2008
 - NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- NIST SP 800-92, *Guide to Computer Security Log Management*, September 2006
 - NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

8. ROLES AND RESPONSIBILITIES

Senior Agency Information Security Officer (SAISO)

- a. The SAISO has the following responsibilities with respect to system and information integrity:
 - i. Carries out the Chief Information Officer security responsibilities under FISMA and serving as the primary liaison for the CIO to the organization's Authorizing Officials, System Owners, Common Control Providers, and Information Security Officers.
 - ii. Possesses professional qualifications, including training and experience, required to administer the information security program functions, and maintains information security duties as a primary responsibility.
 - iii. Heads an office with the mission and resources to assist the organization in achieving more secure information and information systems in accordance to FISMA requirements.

Computer Security Incident Response Capability (CSIRC)

- a. CSIRC has the following responsibilities with respect to system and information integrity:
 - i. 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.
 - ii. Assess and assign priority to alerts, advisories, and directives for remediation actions.
 - iii. Determine appropriate lists for distribution of alerts, advisories, and directives to include at a minimum (i) the SAISO, (ii) primary and backup Information Security Officers (ISOs), (iii) Information System Security Officers (ISSOs), (iv) appropriate information system management and administration personnel.
 - iv. 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.
 - v. Analyze issues associated with application of remediation actions for management resolution.

Office of General Counsel (OGC)/Privacy Act Officer (PAO)

- a. The OGC/PAO has the following responsibilities with respect to system and information integrity:
 - i. 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

- a. FOIA Officials have the following responsibilities with respect to system and
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

information integrity:

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

System Owner (SO)

- a. The SO has the following responsibilities with respect to system and information integrity:
 - i. Provides procurement, development, integration, modification, operation, maintenance, and disposal of an information system.
 - ii. Provides operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements).
 - iii. Provides the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls.
 - iv. Responsible for deciding who has access to the system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior).
 - v. Reviews security assessment results from the Security Control Assessor.

Information Security Officers (ISO) and Managers

- a. ISOs and Managers have the following responsibilities with respect to system and information integrity:
 - i. Maintain an inventory of all components of their information system.
 - ii. Monitor and check for security alerts, advisories, and directives on an ongoing basis for all non-standard components of their information system.
 - iii. Ensure appropriate prioritization of remediation for non-standard IT resources.
 - iv. Respond to alerts, advisories, and directives related to components of the information systems by taking appropriate remediation actions within established time frames.
 - v. Report any issues associated with application of remediation actions to CSIRC.
 - vi. Assign individuals to test remediations of information system components.
 - vii. Train individuals assigned to test information system components as needed.
 - viii. Maintain distribution lists for alerts, advisories, and directives.
 - ix. Distribute alerts, advisories, and directives to information system users as appropriate or requested.
 - x. Consider carefully the structure and content of error messages that are custom developed for an information system component.
 - xi. Configure the information system to prevent non-privileged users from
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

circumventing malicious code protection capabilities.

- xii. Configure the information system to prevent non-privileged users from circumventing intrusion detection and prevention capabilities.

Information System Security Officer (ISSO)

- a. The ISSO has the following responsibilities with respect to system and information integrity:
 - i. Assist information system owners and managers in carrying out their responsibilities.
 - ii. Assist in verifying that remediation actions have been successful.
-

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 – an instance of an information type.
 - 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 disks, digital video disks. 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
-

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

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).
 - Spyware – software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
 - Vulnerability – weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.
 - 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.
 - 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.
 - Written – or “in writing” means to officially document the action or decision and includes a signature. The documentation can be accomplished manually or electronically.
-

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, OTOP shall coordinate to maintain central repository of all waivers.

EPA Classification No.: CIO-2150.3-P-17.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

Related policy and procedures are available on OEI's Policy Resources website.

<http://intranet.epa.gov/oei/imitpolicy/policies.htm>

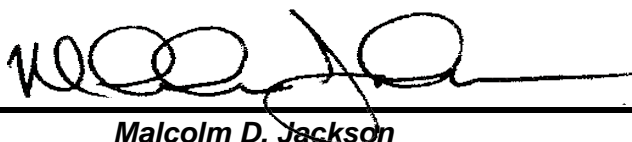
Related standards and guidelines are available on OEI's website.

12. MATERIAL SUPERSEDED

EPA Information Security Manual, Directive 2195A1, 1999 Edition, related parts of Sections 7.2, 8.4, 9.1, 9.2, 9.3, 11.3 and 14

13. ADDITIONAL INFORMATION

NA



Malcolm D. Jackson
Assistant Administrator and Chief Information Officer
Office of Environmental Information

APPENDIX A: ACRONYMS

AO	Authorizing Official
BIOS	Basic Input/Output System
COTS	Commercial-Off-the-Shelf
CSIRC	Computer Security Incident Response Capability
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
FOIA	Freedom of Information Act
GOTS	Government-Off-the-Shelf
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
LSI	Large-Scale Integration
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OGC	Office of General Counsel
OMB	Office of Management and Budget
PAO	Privacy Act Officer
PGP	Pretty Good Privacy
PII	Personally Identifiable Information
SAISO	Senior Agency Information Security Officer
SCAP	Security Content Automation Protocol
SLA	Service Level Agreement
SP	Special Publication
SQL	Structured Query Language
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
USC	United States Code
XML	Extensible Markup Language

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.5	2/16/09	Initial draft	Heather Flager	Procedures-SI-Draft_TO62_020_1
1.0	6/19/09	Incorporated EPA comments Final	Heather Flager	Procedures-SI-Final_TO62_020_2
1.8	8/16/10	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_SI_Draft.T O-062_050_1.0
1.8	8/19/10	TISS Initial review and comments	Charleen Johnson	Procedures_SI_Draft.T O-062_050_1.0
1.9	1/12/10	TISS Final Draft Review	Charleen Johnson	Procedures_SI_Draft.T O-062_050_1.0
2.0	5/1/12	SAISO Final Review	Jabran Malik	Procedures_SI_Draft.T O-062_050_1.0
2.1	7/16/12	Document Review	LaToya Gordon	Procedures_SI_Draft.T O-062_050_1.0