PREFACE TO SELECTED INFORMATION DIRECTIVES

CIO Transmittal No.: 15-010	CIO Approval Date: 06/12/2015

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

CHIEF INFORMATION OFFICER MEMORANDUM

SUBJECT: Chief Technology Officer (CTO) Responsibilities in Selected Information Directives

Re-assigned CTO responsibilities

Effective immediately, CTO responsibilities detailed in the selected information directives (i.e., Information Policies, Procedures, Standards, and Guidance) listed in Appendix A are re-assigned to the OEI Office of Technology, Operations, and Planning (OTOP) Director and the Senior Agency Information Security Officer (SAISO) as detailed. The re-assignment does not change any requirements in the selected information directives.

The OEI Information Directives Program Manager is directed to attach this memorandum and Appendix A as a Preface to each of the Information Directives listed. OEI will then update the Roles and Responsibilities section of each Information Directive in accordance with the normal review and update cycle.

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

APPENDIX A

Information Directive	Prior CTO Responsibilities	Re-assignment
CIO 2104.1 Software Management and Piracy Policy	Provide procedures, standards, and guidance to senior level managers to: support the Agency's Software Management and Piracy Policy and manage enterprise software licenses.	OTOP Director
CIO 2104-P-01.0 Software Management and Piracy Procedure	Provide procedures, standards, and guidance to senior level managers to: support the Agency's Software Management and Piracy Policy, manage enterprise software licenses, and provide covered users within their office with training and awareness on the Software Management and Piracy Policy through the annual Cybersecurity Awareness Training.	OTOP Director
CIO 2121.1 System Life Cycle Management (SLCM) Policy	Establish and publish procedures, technical operational procedures and standards (TOPS), and guidance supporting the Agency's SLCM Policy. Review and approve waivers to the SLCM Procedure.	OTOP Director
CIO 2121-P-03.0 SLCM Procedure	Establish and publish procedures, TOPS, and guidance supporting the Agency's SLCM Policy. Review and approve waivers to the SLCM Procedure.	OTOP Director
CIO 2122.1 Enterprise Architecture (EA) Policy	Issue procedures, guidance, and technical standards associated with the EA with a specific focus on the technology architecture, chair the Quality Technology Subcommittee (QTS), and review technology and security considerations in the Enterprise Target Architecture and Enterprise Transition Plan.	OTOP Director
CIO 2122-P-01.1 EA Governance Procedures	Issue procedures, guidance, and technical standards associated with the EA, with a specific focus on the technology architecture, chair the QTS, and review technology and security considerations in the Enterprise Target Architecture and Enterprise Transition Plan.	OTOP Director
CIO 2122-P-03.0 Information Technology Infrastructure Standard Procedure	Recommend to the CIO a specific IT standard, product or specification to be added to the official Agency IT Standards Profile with consultation from the Quality Information Council (QIC) and the QTS, and develop and maintain the Agency's Technology Architecture.	OTOP Director
CIO 2122-S-02.0 Personal Computer Configuration and Management Standard	Review and approve requests for waivers in regard to this standard.	OTOP Director
CIO 2123.1 Configuration Management Policy	Provide procedures, standards, and guidance to senior level managers in support of the Agency's Configuration Management Policy; institute change management processes; and provide a change management database.	OTOP Director

Information Directive	Prior CTO Responsibilities	Re-assignment
CIO 2150-P-01.1 Information Security - Interim Access Control Procedures	Approve all methods of dial-up access, approve all wireless connections, establish, document, authorize, and monitor all methods of remote access to an information system; delegate to Regions and other entities, as appropriate; and address co-management responsibilities for the Agency Security Architecture.	OTOP Director
CIO 2150-P-08.1 Information Security - Interim Incident Response Procedures	Determine Operational Status Categories during Alerts and Risks (OSCAR) 5 level (page 7).	SAISO
	Be available when the Computer Security Incident Response Capability (CSIRC) must report and coordinate incidents (page 16). Be available to meet with the Director of Cyber Security Staff (CSS) when senior managers are informed of incidents, occurrences and their status (page 18).	OTOP Director
CIO 2150-P-14.1 Information Security - Interim Risk Assessment Procedures	Approve the use of and, as appropriate, acquire and deploy enterprise vulnerability management technology. Consult with the SAISO to determine the coverage and compliance of enterprise vulnerability management technology with respect to federal and Agency requirements, including use of these tools to meet assessment requirements of other control families in NIST 800-53A, Revision 1, and to ensure the most cost effective, complete and accurate results.	OTOP Director
CIO 2150-P-15.1 Information Security - Interim System Services Acquisition Procedures	For the procurement of external information system services where a sufficient level of trust cannot be established, be available to confer regarding risks associated with the network and the Agency.	OTOP Director
CIO 2150-P-16.1 Information Security - Interim System and Communications Protection Procedures	Approve use of mobile VoIP-enabled units.	OTOP Director
CIO 2150.4 Mobile Computing Policy	Oversee policy and procedure implementation regarding use of mobile computing technologies. Approve mobile computing technology and device deployment.	OTOP Director
CIO 2150-P-01.1 Mobile Computing Management Procedures	Oversee policy and the implementation of the procedures. Approve enterprise mobile device types to be deployed. Review and approve requests for waivers in regards to the procedures.	OTOP Director

EPA INFORMATION PROCEDURES

OFFICE OF ENVIRONMENTAL INFORMATION

EPA Classification No.:	CIO-2150.3-P-14.1	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 RISK ASSESSMENT PROCEDURES

V 3.4

JULY 17, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Risk Assessment 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 operations 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 operations 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 risk assessment family of controls found in NIST SP 800-53, Revision 3.

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) 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*", November 2000
- Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 2001
- 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
- EPA Information Security Program Plan
- EPA Information Security Program Policy

6. PROCEDURES

RA- 2 – Security Categorization

a. The information and information system must be categorized in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
    i. The authorization boundary is a prerequisite and must be clearly defined before beginning the security categorization.
    ii. The security categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.
    iii. NIST SP 800-60, Revision 1, Volumes 1 and 2 must be used as guidance for the security categorization process.

Note: The security categorization process facilitates the creation of an inventory of information assets, and in conjunction with CM-8, a mapping to the information system components where the information is processed, stored, and transmitted. Refer to Section 9 for a definition on security categorization.

b. The following potential adverse impacts must be considered:

  i. Impacts to other organizations.

  ii. National-level adverse impacts, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives.

c. The full security categorization results, and supporting rationale, must be documented and included in the System Security Plan (SSP) for the information system.

  i. If Privacy Act information is processed, stored, or transmitted by the information system, the system categorization documentation for that information and information system must accurately reflect this fact.

    - A System of Records Notice (SORN) and designated number must also be identified in the SSP.

  ii. Categorization information must be consistent and coordinated with information found in EPA's official inventory system (i.e., READ) and Capital Planning, Investment Control (CPIC) documentation and the Agency's FISMA reporting and tracking system.

d. The security categorization process must be conducted as an organization-wide activity.

  i. The programmatic Information Owner (IO), related staff, management, mission owner, System Owner (SO), and information security staff knowledgeable in the information created or collected by the program shall assist with the development of the security categorization and the organization's mission requirements and responsibilities.

  ii. The Chief Information Officer (CIO) and Senior Agency Information Security Officer (SAISO) must be involved to provide a perspective of Agency-wide risk management.

  iii. Other SOs need to be apprised of and even involved with the security categorization of an information system, if they are responsible for any of the following:

    - A General Support System (GSS) that the information system relies upon.
    - A Major Application (MA) that inherits controls from the information system.
    - An interconnected system or system that shares information with the information system.

e. Security categorization must be part of the system development life cycle (SDLC) as described in NIST SP 800-64, Revision 2. The security categorizations must be:

i. Developed early in the initiation stage to ensure that the appropriate controls can be planned and implemented throughout the SDLC.

- The results of information and information system categorization must be used to identify the initial or baseline security controls as identified in NIST SP 800-53, Revision 3.

ii. Reviewed and updated throughout the life cycle stages prior to security authorization and when changes occur in the information being processed in the information system. Categorization is reviewed in and, therefore, must be correct for the assessment process to ensure a valid authorization.

iii. Reviewed at least annually after security authorization, and updated if necessary.

- The document review history of the annual system categorization must be updated to reflect the date the review was performed.

iv. Reviewed and updated if necessary whenever there is a change in the information processed in the information system, including adding, altering, or removing information.

- Any categorization changes may require modifications of controls, revision of risk assessments and additions to the Plan of Action and Milestones (POA&Ms), including possibly security re-authorization.

f. Information system categorizations must be reviewed and approved by management officials using the following guidelines:

i. Throughout the development life cycle to ensure the categorization is current and reflective of the information being considered for processing in the information system.

ii. At least annually or upon implementation of the information system.

iii. Whenever there is a change in the information processed in the information system, including adding, altering, and removal of information.

g. Proper security categorization must rely upon accurate and complete analysis of the programmatic/mission information stored, processed, or transmitted by the information system.

h. The information must be associated to one or more information types as defined in the Federal Enterprise Architecture Business Reference Model (FEA BRM) and the Agency BRM.

i. If additional information types are identified that are not defined in the FEA BRM or Agency BRM, consultation with the SAISO must occur to ensure that the appropriate information security categorization is identified (in accordance with FIPS 199); and is published.

i. For each information type, the potential impact on confidentiality, integrity and availability of the information (i.e., the three (3) FIPS 199 security objectives) must be determined in order to establish an appropriate security category (i.e., high, moderate, or low) for that information type.

j. EPA defines eight (8) major classes of information where confidentiality may be impacted:

i. Confidential Business Information (CBI).

ii. Confidential Agency Information (CAI).

iii. Privacy Act information.

iv. Personally Identifiable Information (PII).

v. Enforcement-confidential information.

vi. Budgetary information prior to OMB release.

vii. Other information that is exempt from disclosure under the Freedom of Information Act (FOIA).

viii. Controlled Unclassified Information (CUI).

k. Any information system processing PII associated with a Privacy Act System of Records or containing sensitive PII must have a system categorization of moderate or high in accordance with special factors affecting the confidentiality impact level identified in NIST SP 800-60, Revision 1.

l. The highest categorization—also known as the high water mark—determines the overall security categorization for the information system.

i. Applications with a security categorization of moderate or high are considered *de facto* major applications.

ii. Applications with a security categorization of low are generally not considered major applications, but must be specifically identified in the associated GSS SSPs.

m. When an information system—typically, a GSS—provides security or processing capabilities for one or more other information systems, then the highest security categorization level of any supported system must also be applied to the system that provides security or processing capabilities. For example, if a moderate GSS provides security or processing capability for an application categorized as high, then the GSS must also be categorized as high.

n. For nationally deployed information systems, the FIPS 199 security categorization must be established by the EPA program or regional organization responsible for the information system and must be monitored and updated, as needed, during the system's life cycle.

o. For systems containing PII, the confidentiality security objective shall be assigned an impact level of moderate or higher.

p. Subsystems may be categorized independently and associated controls applied as required by the categorization, provided that:

i. An adequate guard system and other controls are employed between the subsystems to maintain security of the subsystem in a higher category.

ii. The criticality and impact(s) on the information and of the subsystem's interrelationships are assessed considering:

- The sharing, exchange, transfer, or other transaction of information between subsystems.
- The categorization level of each information type's security goals involved between subsystems.

iii. The results of this analysis indicate there is no impact or the impacts are adequately mitigated and documented. The analyses determine the following:

- There is no impact on availability of the information type involved in a transaction in a subsystem at a higher categorization level with a subsystem of the lower categorization level; or
- An information life cycle event occurs, such as approval of pre-solicitation information for inclusion in a contract solicitation that permits the information to be transferred to a publicly accessible subsystem from a confidentiality protected subsystem.

iv. Such a scoping or separation of subsystem's categorization provides an overall cost benefit to the information system as a whole.

q. The security categorization decision must be reviewed and approved by the Authorizing Official (AO) or AO designated representative.

<u>RA- 3 – Risk Assessment</u>

a. Assessments must be conducted to evaluate the level of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

i. The authorization boundary is a prerequisite and must be clearly defined before beginning the risk assessment.

b. The Risk Assessment must take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk to organizational operations, organizational assets, individuals, other organizations, or the Nation.

i. The Risk Assessment must take into account risks posed to EPA's operations, EPA's assets, or individuals from external parties, including but not limited to:

- Entities such as foreign nations and business competitors that may have an interest in information supplied to EPA.
- Service providers.
- Contractors operating information systems on behalf of the Agency.
- Individuals accessing EPA's information systems.
- Outsourcing entities.

ii. The Risk Assessment must address public access to federal information systems and include risks associated with electronic authentication, if this is applicable.

- In accordance with OMB policy and related e-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information.
- Refer to *Information Security – Identification and Authentication*

Procedures for guidance on performing e-authentication risk assessments.

iii. The Risk Assessment must factor in incident information, results and trends of continuous monitoring, penetration testing, and vulnerability scanning efforts.

iv. The Risk Assessment must factor in the status of POA&Ms for the information system.

v. The Results after completing a Risk Assessment should be documented in the Risk Assessment Report (RAR).

c. Risk assessments must be a collaborative effort among representatives of management, operational, technology and information security disciplines.

d. NIST SP 800-30 must be used as guidance on conducting risk assessments.

e. The risk assessment results must be documented in the Risk Assessment Plan or the System Security Plan.

f. The system Risk Assessment must be reviewed and updated annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

g. The following are the specific criteria (but not limited to these criteria) for what is considered a significant change to the information system:

i. A change to the operating environment of a major information system that alters the overall level of risk previously authorized by the AO.

ii. A change to the threat environment.

iii. A change in the IT system's physical environment.

iv. A significant change to the software or hardware.

v. A breach of the information system's security that could possibly invalidate the authorization.

vi. A change with respect to interconnected systems.

vii. A change in the security categorization level.

h. The Risk Assessment must be reviewed and, if necessary, updated:

i. As part of the change management activities for the information system.

- Refer to *Information Security – Configuration Management Procedures* for requirements on change management.

ii. At least annually.

i. The document review history of the Risk Assessment must be updated to reflect the date the review was performed.

j. The results of the annual review must be reported to the AO.

k. Risk Executives shall review recommendations for risk determinations and risk acceptability and may recommend changes to the AO and appropriate CIO.

l. If at any time during the risk assessment a threat or vulnerability that presents a critical risk to the system or its assets is uncovered, that threat or vulnerability must be brought to the immediate attention of the SO for corrective or mitigating action.

i. A POA&M must be created for the corrective action.

ii. The changes documented in the POA&M must be implemented.

iii. A follow-up analysis must be conducted to determine whether the changes made adequately mitigate the vulnerabilities.

Note: Risk assessments (either formal or informal) can be conducted by organizations at various steps in the Risk Management Framework including: information system categorization; security control selection; security control implementation; security control assessment; information system authorization; and security control monitoring. RA-3 is a noteworthy security control in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the tailored baselines with additional security controls or control enhancements.

m. The following sections must be included in the Risk Assessment:

i. System Characterization

- It is a description of the information system that includes its purpose, business need, and functions or functional requirements; the types of users; its FIPS 199 security categorization; whether it is a GSS or MA; the system boundaries and the technical environment or architecture; interfaces and interconnections with other systems; the physical, environmental, and operational environment;
- The purpose of the system characterization is to define the scope of the Risk Assessment and provide all relevant information that affects risks to the system.

ii. Control Review – Vulnerabilities

- Each control required by NIST SP 800-53, Revision 3 must be listed, including the implementation status (i.e., not in place, planned, in place) of the control.
- Controls that are in place may be tentatively considered to be of low risk pending further analysis.
- Controls that are either planned or not in place must be considered to have at least moderate or high risk since they constitute vulnerabilities.
- If a baseline security requirement does not provide adequate security for the IT system or does not reduce the level of risk to an acceptable level, additional controls or enhancements required to further mitigate or reduce the risk to an acceptable level must be identified.
- Other vulnerabilities may be identified from a variety of sources, such as information security tests; published reports of vulnerabilities; audit findings; etc.

  - Each facility and organizational unit shall maintain current information or lists on known system vulnerabilities, system flaws, and weaknesses that could be exploited by the threat sources.

iii. Threats

- Threat(s) must be identified for each vulnerability, thus creating a vulnerability/threat pair.
- The threat sources for each threat must be identified and analyzed in terms of threat actions and potential consequences.

iv. Likelihood

- The likelihood that a threat will be exercised against the vulnerability must be identified for each vulnerability.
- The likelihood must at least be expressed in qualitative terms such as high, medium, or low.
- The likelihood may be expressed in quantitative terms (e.g., on a scale of one (1) to five (5) or as a statistical probability).

v. Impact Analysis (not to be equated with impact in FIPS 199)

- The impact analysis assesses the potential adverse consequences of a threat being exercised for an identified vulnerability.
- The impact analysis must consider:
  - The mission or business impact analysis (BIA) of the functions of the organization supported by the system and its information.
  - The criticality (i.e., importance to the organization) and sensitivity of both the information system and its information. This is evaluated in terms of each of the three security objectives (i.e., confidentiality, integrity, and availability) that are part of the security categorization.
  - The effect on the information system’s security posture resulting from changes to the system (often during continuous monitoring or operations and maintenance (O&M) phase, but which may occur during design of the system).

vi. Risk Analysis

- For each vulnerability/threat pair, the risk level (i.e., high, medium, or low) must be calculated using the method described in NIST SP 800-30 and documented for the Risk Assessment report.
- The calculated risk levels must be used to prioritize risks and determine which ones justify a recommendation for further mitigating controls.

vii. Control Recommendations

- Controls that can mitigate the identified risks in accordance with the needs of the organization’s operations must be identified.

- Based on the information from the risk analysis, each control must be examined and analyzed to determine if it is adequately protecting the information and information system or if it requires enhancement.
- For all controls that are determined to require enhancement, specific recommended corrective actions must be provided.

viii. Summary

- The results of the assessment must be summarized and documented as part of the Risk Assessment report. This includes the number of high, medium, and low risks, as well as the overall level of system risk.
- The final Risk Assessment report must provide a conclusion that includes an overall risk statement.

n. The risk assessment results must be considered privileged information, to be shared only with authorized individuals.

o. Copies of the Risk Assessment report must be provided to the SAISO and Information Security Officer (ISO) for review and comment. The SAISO or ISO may require additional controls, enhancements, or mitigations as needed.

p. The Risk Assessment report must be presented to the System Owner (SO), the AO, other appropriate IT and physical security directors, and Information System Security Officer (ISSO) for their review and appropriate action.

q. The outstanding risks must also be presented to designated information security personnel and management of related GSSs, MAs, and interconnected systems, if any, since the risks may affect the risk profile of their information system.

r. The AO must be informed if the acceptable level of risk already established for the information system changes.

s. The results of the Risk Assessment must be used as follows:

i. The risk must be considered when scoping the applicability of individual security controls in the control baseline (derived from the security categorization). If a risk-based decision is made, the reasons for doing so must be documented and communicated to appropriate management officials within the organization.

ii. If the information system is in the implementation or the O&M phase of the system life cycle, corrective actions must be undertaken for all moderate and high risks, with the tasks to perform the corrective actions documented in the POA&M for the information system. The implementation description for the associated control must also be updated in the SSP.

iii. If the system is under development and not yet implemented, the implementation descriptions for controls in the SSP must discuss how the risk(s) will be mitigated.

RA- 5 – Vulnerability Scanning

a. EPA shall scan for vulnerabilities in the information system and hosted applications at most every 30 days for a system with a low system categorization. High and Moderate systems shall be scanned weekly and when new vulnerabilities potentially affecting the system/applications are identified and reported.

i. The security categorization of the information system must guide the frequency and comprehensiveness of the vulnerability scans.

ii. Vulnerability scanning must include scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms.

iii. EPA shall consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.

iv. The information system vulnerabilities list shall be updated at least weekly or when new vulnerabilities are released.

Note: The Common Weakness Enumeration (CWE) and the National Vulnerability Database (NVD) are also excellent sources for vulnerability information.

b. Vulnerability scanning and penetration testing must be used to assess the adequacy of security controls for the information system and adherence to federal and Agency requirements.

c. EPA shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.

d. Vulnerability scan reports and results from security control assessments must be analyzed.

Note: Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers).

e. Scanning may be conducted independently or as a coordinated effort with EPA Security Operations Center (SOC) in the National Computer Center (NCC).

f. External testing must be performed by a recognized independent security resource.

i. Testing must, at a minimum, include remote scanning and probing to identify potential exploits and vulnerabilities.

ii. Test results must capture all vulnerabilities and must include recommendations for implementing industry best practices solutions.

iii. Testing must be conducted on specifically identified assets with the advice and consent of the CIO.

g. Vulnerability scanning must be conducted using scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards that:

i. Enumerate platforms, software flaws, and improper configurations.

ii. Format and make transparent, checklists and test procedures.

iii. Measure vulnerability impact.

h. NIST SP 800-40, Version 2 must be used as guidance on patch and vulnerability management.

i. NIST SP 800-115 must be used as guidance on information security testing and assessment.

j. Vulnerability scans must have defined a clear scope for all vulnerability scanning activities and designate knowledgeable and trained individuals to perform the scans. Prior to commencing vulnerability scanning efforts, the following should be addressed:

i. **Scanner selection** – SOs shall evaluate the tools for use within their respective environments.

- The network and host-based vulnerability scanner must provide the following capabilities:
  - Identify active hosts on networks.
  - Identify active and vulnerable services (ports) on hosts.
  - Identify vulnerabilities associated with discovered operating systems and applications.
- EPA shall implement a suite of automated monitoring tools to more effectively monitor and identify vulnerabilities on networked computer servers.

ii. **Purpose –** A vulnerability scan must have a defined purpose. Vulnerability scanning happens periodically, as part of the information system authorization process, and during the risk assessment process. Vulnerability scans are typically performed against all systems and for all known vulnerabilities. While this purpose is suitable for meeting quarterly or semi-annual requirements, the SO shall conduct vulnerability scans to be performed as noted below:

- Regularly scheduled scans must occur at most every 30 days.
- Additional scheduled scans must occur after system updates (e.g., upgrade to the operating system, change to hardware platform) or the identification of a major vulnerability.
- Unscheduled scans may occur when deemed necessary by the ISSO.

iii. **Scope/boundaries** – An active vulnerability scan must have a defined scope or boundary. The scope must be clearly defined in written Rules of Engagement (ROE). The scan must be limited to a specific information system, system(s), subnet(s), or network(s) within the realm of responsibility for EPA.

- If scans will occur outside the realm of responsibility for EPA, then a memorandum of understanding (MOU) must be drafted and signed by the AO of each affected Agency.
- Scans typically should be performed only on production systems and

networks that are known to be stable and preferably during times of least impact to the critical functionality of the system. It is expected that vulnerability scanning will occur during various phases of the system's life cycle.

iv. **Signatures/tests** – Compliance with EPA's configuration standards must be tested. The signatures/tests that will be run against identified scope/boundaries should be selected as appropriate for the purpose of the vulnerability scanning.

v. **Research potential negative impacts** – Once signatures/tests are selected, research should occur to determine if any of those signatures/tests may have a potential negative impact on the scope/boundaries selected.

vi. **Coordination/announcement** – Coordination with and/or notification to the relevant or affected parties, depending on the scope and purpose of the scans, must occur before an active vulnerability scan is performed, especially if that scan may result in a potential negative impact. While EPA may have the realm of responsibility for particular devices or systems, it is prudent to coordinate or notify the SO, system administrators, and all incident detection and response personnel of the scanning, unless non-routine type scans or penetration tests are being performed, in which case the SAISO must be advised to ensure select and appropriate individuals are advised. System administrators can then monitor their systems for potential negative impacts. Any potential negative impact discovered during research must be disclosed before scanning is performed.

- The SO of the system to be scanned shall inform the SOs of any interconnected information systems as required by their interconnection agreement.

k. The following must be addressed before, during, and after the vulnerability scan:

i. **Update scanning software** – Before the vulnerability scan is performed, the vulnerability scanner must be updated with the latest patches and database signatures/tests. Scanners that are not maintained and out of date will not contain the most recent signatures/tests and, as a result, vulnerabilities could be missed. Scans performed by scanners that are not maintained are not valid for meeting the scanning requirements and results cannot be claimed on FISMA reporting or used in the security assessment and authorization process.

ii. **Perform scanning exercise** – The designated personnel shall perform the scan of the network and devices in accordance with the established ROE.

iii. **Verify system availability** – After completing the test, the designated personnel shall check system status directly or by coordinating with the system administration team to ensure that the test did not result in unintended consequences and that the system remains operational.

l. Once the vulnerability scanning has been completed, the results must be analyzed and documented in a vulnerability scan report.

m. Documented scan results, including any discovered deficiencies, must be provided to ISO, SOs, and other appropriate EPA personnel and affected systems, as appropriate or required. Executive summaries must be provided to the ISSO and SIO.

n. The information obtained from the vulnerability scanning process and security control assessments must be shared with SOs and ISOs throughout EPA to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

o. Legitimate vulnerabilities discovered from scans and penetration testing must be remediated; 30 days for highs, 60 days for moderates in accordance with an organizational assessment of risk.

p. The Program Manager shall review, approve, and sign all custom-developed code prior to deployment into production environments. The Program Manager may delegate this authority to another EPA employee in writing. This authority shall not be delegated to contractor personnel.

q. Discovered deficiencies must be added to the system POA&M for correction or mitigation as follows:

    i. **Critical or High Vulnerabilities** – These must be reported immediately when verified. SOs have 30 days to correct these after which a POA&M must be established.

    ii. **Moderate Vulnerabilities** – These must be corrected within 60 days after which a POA&M must be established.

    iii. **Low Vulnerabilities** – These must be corrected after high and moderate vulnerabilities are corrected as time permits. POA&Ms do not need to be established unless an aggregation of these vulnerabilities raises the risk to moderate or high.

r. The following corrective actions must be used when necessary as a result of vulnerability scanning results:

    i. Upgrade or patch vulnerable systems to mitigate identified vulnerabilities as appropriate.

    ii. Deploy mitigating measures (e.g., management, technical, procedural) if the system cannot be immediately patched (e.g., operating system upgrade will make the application running on top of the operating system inoperable) in order to minimize the probability of this system being compromised. Mitigating controls satisfy “correction” of a vulnerability only if no control described in SP 800-53, Revision 3 applies or is available. For example, some vulnerabilities have published “work-arounds” that may suffice until a technical solution is found. These may require an item in the POA&M.

    iii. Improve the change management and configuration management program and procedures and standards to ensure that systems are upgraded routinely with the latest solutions.

    iv. Assign a specified team or person(s) responsible for monitoring vulnerability alerts and mailing lists, examine applicability to the Agency’s environment, and initiate appropriate system changes.

    v. Modify or recommend modifications to the Agency’s security policies, architecture, or other documentation, processes or procedures to ensure that security practices include timely system updates and upgrades.

For moderate and high information systems

s. EPA shall employ vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.

t. EPA shall update the list of information system vulnerabilities scanned prior to each scan or when new vulnerabilities are identified and reported.

u. EPA shall employ vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

v. EPA shall attempt to discern what information about the information system is discoverable by adversaries.

w. EPA shall include privileged access authorization to all EPA information system components for selected vulnerability scanning activities to facilitate more thorough scanning.

x. EPA shall employ automated mechanisms every 30 days to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.

7. RELATED DOCUMENTS

- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002
- NIST SP 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009
- NIST 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, June 2010
- NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, *Volume 1: Guide*, August 2008
- NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume 2: Appendices*, August 2008
- NIST SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008

8. ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO)

a. The CIO has the following responsibilities with respect to risk management:

   i. Provide senior management leadership to the Agency risk management function.

   ii. Consult with SAISO on risk management issues.

iii. Authorize vulnerability scans or penetration tests in non-routine situations (e.g., where Agency response mechanisms are being tested).

<u>Senior Agency Information Security Officer (SAISO)</u>

b. The SAISO has the following responsibilities with respect to risk management:

i. Assist the CIO and CTO in the Agency risk management function.

ii. Review, comment on and consult on the security categorizations.

iii. Review, comment on, and provide recommendation on the Risk Assessment.

iv. Authorize routine vulnerability scans and penetration tests.

v. Conduct and coordinate oversight scans and penetration tests and report results to relevant program and Regional management, the CTO and CIO, as appropriate.

vi. Coordinate with the Office of Inspector General (OIG) Office of Investigations and with United States Computer Emergency Readiness Team (US-CERT) where non-routine vulnerability scanning is planned to ensure federal investigative and response activities are not triggered.

vii. Provide management with risk management information and results of vulnerability scans.

viii. Recommend and approve security vulnerability management products for use in EPA's environment.

<u>Senior Information Official (SIO)</u>

c. The SIO has the following responsibilities with respect to risk management:

i. Consider risk impacts associated with information systems under their management control.

ii. Consult with CIO and SAISO on shared risks and other risk management issues.

iii. Understand risks associated with their systems.

iv. Decide whether to accept risks associated with information systems under their management control.

v. Brief CIO and SAISO on information system risks.

<u>Chief Technology Officer (CTO)</u>

d. The CTO has the following responsibilities with respect to risk management:

i. Approve the use of and, as appropriate, acquire and deploy enterprise vulnerability management technology.

ii. Consult with the SAISO to determine the coverage and compliance of enterprise vulnerability management technology with respect to federal and Agency requirements, including use of these tools to meet assessment requirements of other control families in NIST 800-53A, Revision 1 and to ensure the most cost effective, complete and accurate results.

Office of General Counsel (OGC)

e. The OGC has the following responsibilities with respect to risk management:
   - i. Provide legal advice to the CIO and SAISO regarding vulnerability scanning when needed.

Authorizing Official (AO)

f. The AO has the following responsibilities with respect to risk management:
   - i. Review and approve the security categorization decision.

Information Security Officer (ISO)

g. The ISO has the following responsibilities with respect to risk management:
   - i. Review and provide consultation on security categorizations.
   - ii. Review and assist with the risk assessment.
   - iii. Conduct vulnerability scans as needed and authorized.

System Owner (SO)

h. The SO (e.g., owner of a general support system, application, major application, or other OMB non-reportable application) has the following responsibilities with respect to risk management:
   - i. Coordinate with the information owner regarding risk management activities.
   - ii. Coordinate risk management activities with the owner of the GSS(s), if applicable, which provide or will provide the processing platform(s) and associated security controls for the application.
   - iii. Properly categorize the information system and fully document the categorization in the SSP in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
   - iv. Ensure that the potential impact for each security objective associated with the particular information type has been determined in order to establish an appropriate security category for that information type.
   - v. Ensure that the overall security categorization reflects the high water mark of the information types processed by, stored on, or transmitted by the information system.
   - vi. Consider organization-wide risk with respect to security categorizations.
   - vii. Consider potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts in categorizing the information system.
   - viii. Review security categorizations at least annually.
   - ix. Conduct assessments of the risk, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

x. Review and approve the Risk Assessment for the information system, ensuring business impact assessment(s) have been considered and included.

xi. When changes are made to address critical risks, conduct a follow-up analysis to determine whether the changes adequately mitigate the vulnerabilities.

xii. Review the Risk Assessment at least annually and update the Risk Assessment as required and as part of the information system's security authorization.

xiii. Inform the AO if the acceptable level of risk for the information system changes.

xiv. Evaluate the scanning tools for use within their respective environments.

xv. Coordinate with CSIRC and the SAISO regarding Rules of Engagement, and all scans, and penetration testing to be performed.

xvi. Conduct routine vulnerability scans and continuous monitoring using approved technologies.

xvii. Inform the SOs of any interconnected information systems as required based on their interconnection agreement of any changes to security categorization or changes to risk levels.

Information Owner (IO)

i. The IO has the following responsibilities with respect to risk management:

i. Consider or conduct the security categorizations as an organization-wide activity with the involvement of the SIO, CIO, SAISO, other SOs, mission owners, and IOs, as needed, to ensure organization-wide consistency.

ii. Consider potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts in categorizing the information system.

iii. Analyze the information specific to the program/mission information to provide input into the security categorization of the applicable information system.

iv. Conduct risk and business impact assessments and analyses.

v. Review and approve the security categorization and Risk Assessment.

Information System Security Officer (ISSO)

j. The ISSO has the following responsibilities with respect to risk management:

i. Assist information SO and IO with analyzing security categorization of and risks to their specific EPA program/mission information and information systems.

ii. Conduct and/or review results of vulnerability scans and penetration tests.

iii. Review and assist with risk assessments.

iv. Conduct vulnerability scans as needed and authorized.

v. Provide relevant data or information to authorized personnel for vulnerability scanning.

Computer Security Incident Response Capability (CSIRC)

k. The CSIRC has the following responsibilities with respect to risk management:

i. Monitor outputs and reports of enterprise vulnerability management activities for incidents.

ii. Coordinate vulnerability management activities with the OIG Office of Investigations, as needed.

9. DEFINITIONS

- Authentication – the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- Authorization Boundary – all components of an information system to be authorized by an Authorizing Official and excludes separately authorized systems, to which the information system is connected. Synonymous with the term security perimeter defined in Committee on National Security Systems (CNSS) Instruction 4009 and Director of Central Intelligence Directive (DCID) 6/3.
- Chief Information Officer – an Agency official responsible for:

  i. Providing advice and other assistance to the head of the executive Agency and other senior management personnel of the Agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the Agency.

  ii. Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the Agency.

  iii. Promoting the effective and efficient design and operation of all major information resources management processes for the Agency, including improvements to work processes of the Agency.
- Federal Information System – an information system used or operated by an executive Agency, by a contractor of an executive Agency, or by another organization on behalf of an executive Agency.
- General Support System (GSS) - an interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example, can be a: (i) LAN including smart terminals that support a branch office; (ii) backbone (e.g., Agency-wide); (iii) communications network; (iv) Agency data processing center including its operating system and utilities; (v) tactical radio network; or (vi) shared information processing service facility. A general support system can have a FIPS 199 impact level of low, moderate, or high in its security categorization, depending on the criticality or sensitivity of the system and any major applications the general

support system is supporting. A general support system is considered a major information system when special management attention is required; there are high developments, operating, or maintenance costs; and the system/information has a significant role in the administration of Agency programs. When the general support system is a major information system, the system's FIPS 199 impact level is either moderate or high.

- Information - an instance of an information type.
- Information Owner – an official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
- Information Security – the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- Information Security Policy – an aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.
- Information System – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- Information Technology – any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive Agency. For purposes of the preceding sentence, equipment is used by an executive Agency if the equipment is used by the executive Agency directly or is used by a contractor under a contract with the executive Agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
- 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.
- Major Application - an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.
- Organization – a federal Agency or, as appropriate, any of its operational elements.
- Penetration Testing – security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real

systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

- Potential Impact – the loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
- 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.
- Risk Assessment – the process of identifying risks to Agency operations (including mission, functions, image, or reputation), Agency assets, individuals, other organizations, and the Nation arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in place security controls.
- Risk Management – the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
- Security Categorization - describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be compromised through a loss of confidentiality, integrity, or availability
- 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.
- System Owner – official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
- 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.
- Threat Source – the intent and method targeted at the intentional exploitation of vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
- User – individual or (system) process authorized to access an information system.
- Vulnerability – weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.
- Vulnerability Assessment – formal description and evaluation of vulnerabilities of an

information system.

- Vulnerability Scanning – a technique used to identify hosts/host attributes and associated vulnerabilities.
- 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.

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, Section 4.0 and related topics in Sections 3.0 and 9.3

13. ADDITIONAL INFORMATION

NA

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

APPENDIX A: ACRONYMS

AO	Authorizing Official
BIA	Business Impact Analysis
BRM	Business Reference Model
CAI	Confidential Agency Information
CBI	Confidential Business Information
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CPIC	Capital Planning and Investment Control
CSIRC	Computer Security Incident Response Capability
CTO	Chief Technology Officer
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DCID	Director of Central Intelligence Directive
EPA	Environmental Protection Agency
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GSS	General Support System
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
MA	Major Application
MOU	Memorandum of Understanding
NCC	National Computer Center
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OGC	Office of General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
OVAL	Open Vulnerability Assessment Language
O&M	Operations and Maintenance
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
ROE	Rules of Engagement
SIO	Senior Information Official
SO	System Owner
SP	Special Publication
SOC	Security Operations Center
SORN	System of Records Notice
SSP	System Security Plan
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team

DOCUMENT CHANGE HISTORY

Versio n	Release Date	Summary of Changes	Author of Changes	DCN
0.5	12/5/2008	Initial draft	Heather Flager	Procedures-RA-Draft_TO62_020_1
2.0	5/6/2009	Incorporated EPA comments Final	Heather Flager	Procedures-RA-Draft_TO62_020_2
2.1	5/7/2009	Edits in RA-2	William Gill	Procedures_RA_Final_v2.1.doc
2.2	9/22/2009	Added Senior Agency Official responsibilities and amended SIO	William Gill	Procedures_RA_Final_v2.2.doc
3.1	8/16/2010	Updated per NIST SP 800-53 Revision 3	Heather Flager	Procedures_RA_Draft.TO-062_050_1.0
3.1	8/19/2010	TISS Initial review and comments	Charleen Johnson	Procedures_RA_Draft.TO-062_050_1.0
3.2	12/27/2010	TISS Final Draft Review	Charleen Johnson	Procedures_RA_Draft.TO-062_050_1.0
3.3	4/27/2012	SAISO Final Review	Jabran Malik	Procedures_RA_Draft.TO-062_050_1.0
3.4	7/17/2012	Document Review	LaToya Gordon	Procedures_RA_Draft.TO-062_050_1.0