INFORMATION PROCEDURE

Information Security – Risk Assessment Procedures	
EPA Classification No.: CIO 2150-P-14.2	CIO Approval Date: 4/11/2016
CIO Transmittal No.: 16-007	Review Date: 4/11/2019

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

INFORMATION SECURITY – RISK ASSESSMENT PROCEDURES

1. PURPOSE

To implement the security control requirements for the Risk Assessment (RA) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

2. SCOPE AND APPLICABILITY

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

The 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

The audience is 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 shall meet the security requirements for the security controls defined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* as amended. This document addresses the procedures and standards set forth by the EPA, and complies with the family of Risk Assessment controls.

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act (FISMA) as amended.

- Federal Information Security Modernization Act of 2014, Public Law 113-283, Chapter 35 of Title 44, United States Code (U.S.C.).
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996.
- Clinger-Cohen Act of 1996, Public Law 104-106.
- Paperwork Reduction Act of 1995 (44 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.
- EPA Information Security Roles and Responsibilities Procedures.
- EPA Information Security Continuous Monitoring Strategic Plan.
- CIO Policy Framework and Numbering System.

6. PROCEDURES

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

Abbreviations including acronyms summarized in Appendix A.

RA- 2 – Security Categorization

For All Information Systems:

1) The System Owners (SO), in coordination with Information Owners (IO), Information System Security Officers (ISSO), Senior Agency Information Security Officer (SAISO), Information Security Officers (ISO), and Authorizing Officials (AO), for EPA-operated systems, shall; and

Service Managers (SM), in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:[1]

a) Categorize the information and information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.
   i) The information system (IS) authorization boundary is a prerequisite and shall be clearly defined before beginning the security categorization decision process.
   ii) NIST SP 800-60, Revision 1, Volumes 1 and 2 serve as guidance for the security categorization process. The security categories are based on the potential impact on an organization should certain events occur that jeopardize the confidentiality, integrity, and availability of 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) The following potential adverse impacts shall be considered during the security categorization process:
      (1) Impacts to EPA, personnel, other organizations and the nation.
   iv) Conduct the security categorization process as an organization-wide activity.
   v) The programmatic IO, related staff, management, mission 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.
   vi) The Chief Information Officer (CIO) and Senior Agency Information Security Officer shall provide an Agency-wide risk management perspective through the Enterprise Risk Management Process (ERMP).
   vii) Other SOs need to be apprised of and involved with the security categorization of an information system if they are responsible for any of the following:
      (1) A system that the information system relies upon.
      (2) A system that inherits controls from the information system.
      (3) An interconnected system or system that shares information with the information system.
   viii) Include the security categorization process as a part of the system development life cycle (SDLC) as described in NIST SP 800-64. The security categorizations shall be:
      (1) Developed early in the initiation stage ensuring the planning and implementation of the appropriate security controls throughout the SDLC.
      (2) The results of information and information system categorization identify the initial or baseline security controls as identified in the current version of NIST SP 800-53.

[1] *Validate Service Providers' controls through independent assessments in accordance with FedRAMP. Information Owners and Service Managers ensure controls are in place and operating as intended by reviewing documentation provided by Service Providers and FedRAMP. Authorizing Officials may accept provisional authorizations to operate issued by FedRAMP because of review by the combined DoD, GSA & DHS process without reviewing supporting documentation. Review supporting documentation for all other provisional authorizations to operate before acceptance.*

(3) Reviewed and updated throughout the SDLC stages prior to authorization test or operate and when changes occur in the information types or risk levels. Review and update, as necessary, in the System Security Plan (SSP) as correct for the assessment process to ensure a valid authorization.

(4) Reviewed at least annually after security authorization, and updated as necessary.

(5) Update the document review history of the annual system categorization to reflect the date the review performed.

ix) Reviewed and updated as necessary whenever there is a change in the information processed by the information system, including adding, modifying or removing information.

x) 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.

xi) Proper security categorizations rely upon accurate and complete analysis of the programmatic/mission information stored, processed or transmitted by the information system.

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

xiii) Additional information types identified not defined in the FEA BRM or Agency BRM, consultation with the SAISO shall occur to ensure that the appropriate information security categorization, in accordance with FIPS 199, assigned and updated in the IS SSP.

xiv) For each information type, the potential impact on confidentiality, integrity, and availability of the information shall be determined in order to establish an appropriate security category (High, Moderate, or Low) for that information type.

xv) Per FIPS 199, the highest security mark for each information type —also known as the high water mark—determines the overall security categorization for the information system.

xvi) National Archives and Records Administration (NARA) designates specific information categories[2] as Controlled Unclassified Information (CUI), consistent with the guidance EPA shall apply appropriate controls to protect against the unauthorized dissemination of CUI.

xvii) Any information system processing PII associated with a Privacy Act System of Records or containing sensitive PII shall 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.

xviii) When an information system provides security or processing capabilities for one or more other information systems, then the highest security categorization level of

[2] *Refer to the National Archives web site: http://www.archives.gov/cui/registry/cui-glossary.html for guidance and definition.*

any supported is applied to the system that provides security or processing capabilities. For example, if a Moderate system provides security or processing capability for an application categorized as High, then the Moderate-categorized system level changes to High.

xix) For nationally deployed information systems, the FIPS 199 security categorization established by the EPA Program or Regional organization responsible for the information system shall be monitored and updated, as needed, during the system's life cycle.

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

(1) An adequate guard system and other controls employed between the subsystems maintain security of any subsystem in a higher category.

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

(a) The sharing, exchange, transfer, or other transaction of information between subsystems.

(b) The categorization level of each information type's security goals involved between subsystems.

(c) The results of this analysis indicate either there is no impact or the impacts are adequately mitigated and documented.

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

Note: The security categorization process facilitates the creation of an inventory of information assets, and in conjunction with security control 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) Document categorization results (including supporting rationale) in the IS security plan.

i) Conduct and document the results of the annual review of the system categorization with date generated as an artifact in the Agency Information Security Repository and generate an updated SSP reflecting the system categorization review.

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

iii) Identify the System of Records Notice (SORN) and designated number in the SSP.

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

c) Ensure that the AO or the AO-designated representative reviews and approves the security categorization decisions.

RA- 3 – Risk Assessment

For All Information Systems:

1) SOs, in coordination with Senior Information Officials (SIO), IOs, ISSOs, SAISO, ISOs, and AOs, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Conduct a risk assessment (RA)[3] 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 IS authorization boundary is a prerequisite for the risk assessment and shall be clearly defined before beginning the risk assessment.
      ii) The risk assessment takes into account threats, vulnerabilities, likelihood and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems.
      iii) The risk assessment takes into account risks posed to EPA's operations, EPA's assets, or individuals from external parties, including but not limited to:
         (1) Entities such as foreign nations and business competitors that may have an interest in information supplied to EPA.
         (2) Service providers:
            (a) Contractors operating information systems on behalf of the Agency;
            (b) Individuals accessing EPA's information systems; and
            (c) Outsourcing entities.
      iv) The risk assessment addresses public access to federal information systems and includes risks associated with electronic authentication, if this is applicable.
      v) In accordance with OMB policy and related e-authentication initiatives,[4] authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information.
      vi) Consider the risk when scoping the applicability of individual security controls in the control baseline derived from the security categorization. When making a risk-based decision, document the reasons and communicate to the appropriate management officials within the organization.
      vii) If the information system is in the implementation or the operational and maintenance (O&M) phase of its system life cycle corrective actions shall be undertaken for all risks, with the tasks to perform the corrective actions documented in the POA&M for

[3] *Refer to EPA's Risk Management Strategic Plan FY 2014, addresses how the Agency will frame risk, assess risk, respond to risk, and monitor risk, which describes the Enterprise Risk Management Process (ERMP).*

[4] *Refer to Information Security Policy – Identification and Authentication Procedures for guidance on performing e-authentication risk assessments.*

the information system. Update the implementation description for the associated control in the IS SSP.

viii) If the system is under development and not yet implemented, the implementation descriptions for controls in the SSP shall discuss how to mitigate risk(s).

ix) 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.

(1) Refer to *Information Security Policy – Identification and Authentication Procedures* for guidance on performing e-authentication risk assessments.

x) The risk assessment shall factor in:

(1) Incident information, results and trends of continuous monitoring, penetration testing, and vulnerability scanning efforts; and

(2) The status of POA&Ms for the information system.

xi) Risk assessments are a collaborative effort among representatives of management, operational, technology and information security disciplines.

xii) Use NIST SP 800-30 for guidance on conducting risk assessments of federal information systems and organizations, amplifying the guidance in NIST SP 800-39.

b) Document risk assessment results in a Risk Assessment Report (RAR).

i) The following sections are included in the Risk Assessment Report:

(1) System Characterization

(a) The system categorization is a description of the information system that includes: its purpose; business needs, functions and functional requirements; the types of users; the FIPS 199 security categorization; the system boundaries, the technical environment and architecture; interfaces; interconnections with other systems; the physical, environmental; and operational environment.

(b) The purpose of the system characterization is to define the scope of the Risk Assessment and provide all relevant information affecting risks to the system.

(2) Control Review – Vulnerabilities

(a) Each control required by the current version of NIST SP 800-53 shall be listed, including the implementation status (e.g., not in place, planned, or in place) of the control.

(b) Controls that are “in place” constitute no risk.

(c) Controls whose implementation status is “planned” or “not in place” result with a risk level that is applicable to the vulnerability and the threat level.

(d) If a baseline security requirement does not provide adequate security for the IT system or information or does not reduce risk to an acceptable level, identify additional controls or enhancements required to further mitigate or reduce the risk to an acceptable level.

(e) Identify potential vulnerabilities from a variety of other sources, such as information security tests, published reports of vulnerabilities, and audit findings.

(3) Threats

(a) Identify threats for each vulnerability, thus creating a vulnerability/threat pair.

(b) Identify and analyze threat sources for each threat in terms of threat actions and potential consequences.

(4) Likelihood

(a) Identify the likelihood of exercising an identified threat against each vulnerability/threat pair.

(b) Express the likelihood:

(i) In qualitative terms such as high, medium, or low; or

(ii) In quantitative probability terms such as on a scale of one (1) to five (5) or as a statistical probability.

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

(a) The impact analysis assesses the potential adverse consequences of a threat exercised for an identified vulnerability.

(b) The Impact Analysis shall consider:

(i) The mission and the business functions of the organizations supported by the system and its information.

(ii) The criticality, (i.e., importance to the organization) and sensitivity of both the IS and its information is evaluated in terms of each of the three security objectives—confidentiality, integrity, and availability—that are part of the security categorization.

(iii) The effect on the information system's security posture resulting from changes to the system, often during continuous monitoring or the operations and maintenance (O&M) phase, but which may occur during design of the system.

(6) Risk Analysis

(a) For each vulnerability/threat pair, calculate the risk level (high, medium, or low) using the method described in NIST SP 800-30 and document it in the Risk Assessment Report.

(b) Use the calculated risk levels to prioritize risks and determine which ones justify a recommendation for further mitigating controls.

(7) Control Recommendations

(a) Identify controls that can mitigate the identified risks in accordance with the needs of the organization's operations.

(b) Based on the information from the risk analysis, examine and analyze each control to determine if the control is adequately protecting the information and information system or if it requires enhancement.

(c) For all controls that are determined to require enhancement, provide specific recommended corrective actions.

(8) Summary

(a) Summarize and document the results of the assessment 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.

(b) The final Risk Assessment Report will provide a conclusion that includes an overall risk statement.

c) Update the Risk Assessment Report at least 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 affecting the security state of the system.

RA-4 – Risk Assessment Update

Incorporated into RA-3.

RA- 5 – Vulnerability Scanning

For All Information Systems:

1) SOs, in coordination with the National Computer Center (NCC) Security Branch, the Network Security Operations Center (NSOC) Vulnerability Management Team (VMT), the SAISO, ISOs, ISSOs, SIOs, the Office of General Counsel (OGC), and the Computer Security Incident Response Capability (CSIRC), for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Conduct vulnerability scans on the information system and hosted applications at least every 72 hours and when new vulnerabilities potentially affecting the system/applications are identified and reported.

b) Ensure the security categorization of the information system guide the frequency and comprehensiveness of the vulnerability scans.

i) Vulnerability scanning shall 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.

(1) Personnel shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches and updates, and eliminating or disabling unnecessary services.

ii) EPA shall use where possible 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.

iii) Update and review vulnerability definitions and signatures prior to each scan or when new vulnerabilities are identified or reported.

iv) Conduct scanning independently or as a coordinated effort with EPA NSOC VMT in the NCC.

v) Prior to commencing vulnerability scanning efforts, the following should be addressed:

(1) **Scanner selection** – Evaluate the mandated tools for use within the respective environments.

(a) The network and host-based vulnerability scanner shall provide the following capabilities:

(i) Identify active hosts on networks.

(ii) Identify active and vulnerable services (ports) on hosts.

(iii) Identify vulnerabilities associated with discovered operating systems and applications.

(b) EPA shall implement a suite of automated monitoring tools to more effectively monitor and identify vulnerabilities on networked computer servers.

(2) **Purpose –** A vulnerability scan shall have a defined purpose. Vulnerability scanning happens periodically, as part of the IS authorization process, and during the risk assessment process. Perform vulnerability scans, typically, against all systems and for all known vulnerabilities. While this purpose is suitable for meeting quarterly or semi-annual requirements, the SO shall ensure that vulnerability scans are being performed as noted below:

(a) Maximum interval between regularly scheduled scans shall be 72 hours.

(b) Additional scheduled scans shall occur after system updates (e.g., upgrade to the operating system, change to hardware platform) or the identification of a major vulnerability.

(c) Unscheduled scans may occur when deemed necessary by the ISSO.

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

(a) If scans will occur outside the realm of responsibility for EPA, then draft a memorandum of understanding (MOU) for signing by the AO of each affected Agency.

(b) Perform scans, typically, only on production systems and networks known to be stable and preferably during times of least impact to the critical functionality of the system. Expect vulnerability scanning to occur during various phases of the system's life cycle.

(4) **Signatures/tests** – Test compliance with EPA's configuration. Select the signatures/tests that to run against identified scope/boundaries as appropriate for the purpose of the vulnerability scanning.

(5) **Research potential negative impacts** – Research selected signatures/tests to determine if any of those signatures/tests might have a potential negative impact on the scope/boundaries selected.

(6) **Coordination/announcement** – Coordination with and/or notification to the relevant or affected parties, depending on the scope and purpose of the scans, shall 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, coordinate or notify the SO, system administrators, and all incident detection and response personnel of scan schedule, unless non-routine type scans or penetration tests are being performed, in which case the SAISO shall be advised to ensure select and appropriate individuals are advised. System administrators can then monitor their systems for potential negative impacts. Disclose any potential negative impact discovered during research before conducting the planned scans.

(a) The SO of the scheduled system scan shall inform the SOs of any interconnected information systems as required by their interconnection agreement.

vi) Perform external testing by a recognized independent security resource.

(1) Testing, at a minimum, shall include remote scanning and probing to identify potential exploits and vulnerabilities.

(2) Test results shall capture all vulnerabilities and shall include recommendations for implementing industry best practices solutions.

(3) Conduct testing on specifically identified assets with the advice and consent of the CIO.

vii) The following is addressed before, during, and after the vulnerability scan:

(1) Update scanning software – Before performing the vulnerability scan, update the vulnerability scanner 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 and not maintained, are not valid for meeting the scanning requirements and the results cannot be claimed on FISMA reporting or used in the security assessment and authorization process.

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

(3) 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.

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

ix) Discoverable information includes information that adversaries could obtain without directly compromising or breaching the information system.

x) Once the vulnerability scanning is completed, analyze the results and document in a vulnerability scan report.

xi) Take corrective actions once results have been analyzed.

(1) Correction actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the information system to make designated information less relevant or attractive to adversaries.

xii) Refer to NIST SP 800-40 for guidance on patch and vulnerability management.

xiii) Refer to NIST SP 800-115 for guidance on information security testing and assessment.

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

2) SOs, in coordination with the NCC Security Branch, NSOC VMT, the SAISO, ISOs, ISSOs, SIOs, OGC, and CSIRC, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Employ EPA enterprise vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management[5] process by using standards that:

i) Enumerate platforms, software flaws and improper configurations.

ii) Format checklists and test procedures.

iii) Measure vulnerability impact.

b) Analyze vulnerability scan reports and results from security control assessments.

i) Vulnerability scanning and penetration testing is used to assess the adequacy of security controls for the information system and adherence to Federal and Agency requirements.

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).

c) Remediate legitimate vulnerabilities discovered from scans and penetration testing in accordance with an organizational assessment of risk.[6]

i) POA&Ms are developed for the appropriate system or program for discovered deficiencies as follows:

(1) **Critical Vulnerabilities** – mitigate or remediate within two calendar days. If more than two days is required, create a POA&M.

(2) **High Vulnerabilities** – mitigate or remediate within 30 calendar days. If more than 30 days is required, create a POA&M.

[5] *Refer to OEI SOP, Vulnerability Management (VM) Program provides operational guidance and describes recurring activities, responsibilities, tools, the categories of vulnerability scans, the NSOC Vulnerability Management Team (VMT) account maintenance functions and vulnerability remediation supporting EPA's VA program.*

[6] *Refer to EPA's Risk Management Strategic Plan FY 2014, addresses how the Agency will frame risk, assess risk, respond to risk, and monitor risk, which describes the Enterprise Risk Management Process (ERMP).*

(3) **Moderate Vulnerabilities** – mitigate or remediate within 60 calendar days. If more than 60 days is required, create a POA&M.

(4) **Low Vulnerabilities** –Correct within 90 calendar days. If more than 90 days is required, create a POA&M.

d) Share the information obtained from the vulnerability scanning process and security control assessments with SOs and ISOs throughout EPA to help eliminate similar vulnerabilities in other information systems (e.g., systemic weaknesses or deficiencies).

i) Document scan results, including any discovered deficiencies, and provide to ISSO, SOs, and other appropriate EPA personnel and affected systems, as appropriate or required. Executive summaries that include the discovered vulnerabilities and criticality rating shall be provided to the SAISO, ISO and SIO.

ii) The Program Manager reviews, approves and signs all custom-developed code prior to deployment into production environments. The Program Manager may delegate this authority to another EPA employee in writing. The authority may not be delegated to contractor personnel.

RA – 5(1) Vulnerability Scanning | Update Tool Capability

For Moderate and High Information Systems:

1) SOs, in coordination with the NCC Security Branch, NSOC VMT, the SAISO, ISOs, ISSOs, SIOs, OGC, and CSIRC, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Employ vulnerability-scanning tools which includes the capability to readily update the information system vulnerabilities to be scanned.

RA-5(2) Vulnerability Scanning | Update By Frequency / Prior To New Scan / When Identified

For Moderate and High Information Systems:

1) SOs, in coordination with the NCC Security Branch, NSOC VMT, the SAISO, ISOs, ISSOs, SIOs, OGC, and CSIRC, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Update and review vulnerability definitions and signatures prior to each scan or when new vulnerabilities are identified or reported.

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with COs, CORs, SOs, ISOs, and ISSOs, for information system services operated on behalf of the EPA, shall ensure service providers:

a) Update the list of vulnerabilities scanned prior to a new scan.

RA – 5(3) Vulnerability Scanning | Breadth and Depth of Coverage

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with COs, CORs, SOs, ISOs, and ISSOs, for information system services operated on behalf of the EPA, shall ensure service providers:

a) Employ vulnerability-scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

RA – 5(4) – Vulnerability Scanning | Discoverable Information

For High Information Systems:

1) SOs, in coordination with the NCC Security Branch, NSOC VMT, the SAISO, ISOs, ISSOs, SIOs, OGC, and CSIRC, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Determine what information about the information system is discoverable by adversaries and subsequently take applicable corrective action.

RA-5(5) Vulnerability Scanning | Privileged Class

For Moderate and High Information Systems:

1) SOs, in coordination with the NCC Security Branch, NSOC VMT, the SAISO, ISOs, ISSOs, SIOs, OGC, and CSIRC, for EPA-operated systems, shall; and SMs, in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Implement privileged access authorization to all EPA information system components for selected vulnerability scanning activities to facilitate more thorough scanning.

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with COs, CORs, SOs, ISOs, and ISSOs, for information system services operated on behalf of the EPA, shall ensure service providers:
   a) Implement privileged access authorization to all operating systems, web applications, and databases for all scans to facilitate more thorough scanning.

RA - 5(6) Vulnerability Scanning | Automated Trend Analysis

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with COs, CORs, SOs, ISOs, and ISSOs, for information system services operated on behalf of the EPA, shall ensure service providers:
   b) Employ automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.
      i) Include in Continuous Monitoring ISSO digests/reports to Authorizing Official.

RA - 5(7) Vulnerability Scanning | Automated Detection and Notification of Unauthorized Components

Incorporated into CM-8.

RA - 5(8) Vulnerability Scanning | Review Historic Audit Logs

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with COs, CORs, SOs, ISOs, and ISSOs, for information system services operated on behalf of the EPA, shall ensure service providers:

a) Review historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

Note: This enhancement is required for all High vulnerability scan findings. While scanning tools may label findings as High or Critical, the intent of the control is based around NIST's definition of High vulnerability.

RA - 5(9) Vulnerability Scanning | Penetration Testing and Analysis

Incorporated into CA-8.

RA – 5(10) Vulnerability Scanning | Correlate Testing and Analysis

Not selected as part of the control baseline.

RA-6 – Technical Surveillance Countermeasures Survey

Not selected as part of the control baseline.

7. RELATED DOCUMENTS

- NIST Special Publications, 800 series
- EPA Standard Operating Procedure, Office of Environmental information, *Vulnerability Management Program*, February 15, 2014

8. ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO)

1) The CIO has the following responsibilities with respect to risk management:
   a) Provide senior management leadership to the Agency risk management function.
   b) Consult with the SAISO on risk assessment and management issues.
   c) Authorize vulnerability scans or penetration tests in non-routine situations (e.g., where Agency response mechanisms are being tested)

Senior Agency Information Security Officer (SAISO)

1) The SAISO has the following responsibilities with respect to risk management:
   a) Assist the CIO and Director of OTOP in the Agency risk management function.
   b) Review, comment on, and consult on the security categorizations.
   c) Review, comment on, and provide recommendation on the Risk Assessment.
   d) Authorize routine vulnerability scans and penetration tests.
   e) Conduct and coordinate oversight scans and penetration tests and report results to relevant program and Regional management, the CIO and the Director of OTOP, as appropriate.

f) Coordinate with the Office of Inspector General (OIG) Office of Investigations and with United States Computer Emergency Readiness Team (US-CERT) when planning non-routine vulnerability scanning to prevent triggering federal investigative and response activities.

g) Provide management with risk management information and results of vulnerability scans.

h) Recommend and approve security-vulnerability management products for use in EPA operating environments.

Senior Information Official (SIO)

1) The SIO has the following responsibilities with respect to risk management:
   a) Consider risk impacts associated with information systems under their management control.
   b) Consult with CIO and SAISO on shared risks and other risk management issues.
   c) Understand risks associated with their systems.
   d) Decide whether to accept risks associated with information systems under their management control.
   e) Brief CIO and SAISO on information system risks.

Director of Office of Technology Operations and Planning (OTOP)

1) The Director of OTOP has the following responsibilities with respect to risk management:
   a) Approve the use of and, as appropriate, acquire and deploy enterprise-vulnerability management technology.
   b) 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)

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

Authorizing Official (AO)

1) The AO has the following responsibilities with respect to risk management:
   a) Review and approve the security categorization decision.

Information Security Officer (ISO)

1) The ISO has the following responsibilities with respect to risk management:
   a) Review and provide consultation on security categorizations.
   b) Review and assist with the risk assessment.

c) Conduct vulnerability scans as needed and authorized.

System Owner (SO)

1) The SO has the following responsibilities with respect to risk management:
   a) Coordinate with the information owner regarding risk management activities.
   b) 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.
   c) Categorize the information system properly and fully document the categorization in the SSP in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.
   d) 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.
   e) 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.
   f) Consider organization-wide risk with respect to security categorizations.
   g) 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.
   h) Review security categorizations at least annually.
   i) Conduct risk assessments, 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.
   j) Review and approve the risk assessment for the information system, ensuring business impact assessment(s) have been considered and included.
   k) Conduct, when making changes that address critical risks, a follow-up analysis to determine whether the changes adequately mitigate the vulnerabilities.
   l) Review the Risk Assessment at least annually and update the Risk Assessment as required and as part of the information system's security authorization.
   m) Inform the AO if the acceptable level of risk for the information system changes.
   n) Evaluate the scanning tools for use within their respective environments.
   o) Coordinate with CSIRC and the SAISO regarding Rules of Engagement, all vulnerability scans, and penetration testing scheduled.
   p) 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)

1) The IO has the following responsibilities with respect to risk management:

a) 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.
b) 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.
c) Analyze the information specific to the program/mission information to provide input into the security categorization of the applicable information system.
d) Conduct risk and business impact assessments and analyses.
e) Review and approve the security categorization and Risk Assessment.

Information System Security Officer (ISSO)

1) The ISSO has the following responsibilities with respect to risk management:
   a) Assist information SO and IO with analyzing security categorization of and risks to their specific EPA program/mission information and information systems.
   b) Conduct and/or review results of vulnerability scans and penetration tests.
   c) Review and assist with risk assessments.
   d) Conduct vulnerability scans as needed and authorized.
   e) Provide relevant data or information to authorized personnel for vulnerability scanning.

Computer Security Incident Response Capability (CSIRC)

1) The CSIRC has the following responsibilities with respect to risk management:
   a) Monitor outputs and reports of enterprise-vulnerability management activities for security-related incidents.
   b) Coordinate vulnerability management activities with the OIG Office of Investigations, as needed.

National Computer Center (NCC) Security Branch

1) The NCC Security Branch has the following responsibilities with respect to risk management:
   a) Monitor budget and overall oversight of the vulnerability management program.
   b) Review and execute requests for ad-hoc scanning to support EPA's AAA Remote Access services and Firewall Rule Request (FRR) changes.
   c) Procure, maintain and decommission VM equipment, licenses, and support.
   d) Oversee and direct the VM Program and the NSOC Vulnerability Management Team.

Network Security Operations Center (NSOC) Vulnerability Management Team (VMT)

1) The NSOC VMT has the following responsibilities with respect to risk management:
   a) Ensure issues that could affect the operation of the VM scanners are elevated to the contract and federal Security Lead.
   b) Provide input for monthly reports.
   c) Provide continuous support of VM scanners.

d) Monitor the health of the VM infrastructure.

e) Distribute vulnerability and remediation information, (e.g., vulnerability and discovery scan data) to the SAISO, ISOs, ISSOs, SAs and other EPA designated individuals.

f) Provide VM training support to assist ISOs, ISSOs and System Administrators in understanding the scan results and assist with remediation efforts.

g) Verify vulnerability remediation through normal recurring scan process or upon request.

h) Monitor security sources for vulnerability announcements and alerts.

i) Create vulnerability trend reports.

j) Alert NCC Security Branch designee(s) of any previously unidentified systems on the network.

k) Maintain a repository of vulnerability and discovery scans to use for trending, historical and investigative research.

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.
- *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.
- *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. 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.
- *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 conduction 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) – to officially document the action or decision, either manually or electronically, and includes a signature.

10. WAIVERS

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

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

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

The SAISO and the Director of 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.

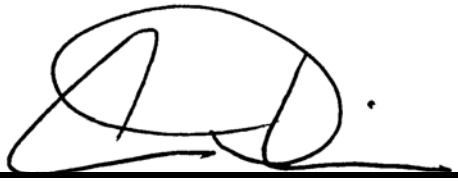
Information Security – Risk Assessment Procedures	
EPA Classification No.: CIO 2150-P-14.2	CIO Approval Date: 4/11/2016
CIO Transmittal No.: 16-007	Review Date: 4/11/2019

12. MATERIAL SUPERSEDED

- EPA Information Procedure: CIO 2150-P-14.1, *Interim Information Security – Risk Assessment Procedures*, July 18, 2012.

13. ADDITIONAL INFORMATION

N/A



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

APPENDIX A: ACRONYMS & ABBREVIATIONS

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
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
IO	Information Owner
IS	Information System
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NCC	National Computer Center
NSOC	Network Security Operations 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
OTOP	Office of Technology Operations and Planning
O&M	Operations and Maintenance
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
RAR	Risk Assessment Report
ROE	Rules of Engagement
SAISO	Senior Agency Information Security Officer
SDLC	System Development Life Cycle

SIO	Senior Information Official
SM	Service Manager
SO	System Owner
SORN	System of Records Notice
SP	Special Publication
SSP	System Security Plan
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team
VMT	Vulnerability Management Team