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

Information Security – Risk Assessment (RA) Procedure

1. PURPOSE

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

The purpose of this procedure is to facilitate the implementation of the EPA security control requirements for the Risk Assessment (RA) control family, as identified in NIST SP 800-53, Revision 5.

2. SCOPE

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

3. AUDIENCE

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

4. AUTHORITY

- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)
- Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource," July 2016
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations, October 2020
- E-Government Act of 2002, Public Law 107-347
- Privacy Act of 1974 (5 USC § 552a) as amended

- NIST SP 800-60 Vol. 1 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
- NIST SP 800-60 Vol. 2 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices, August 2008
- NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments, September 2012

5. PROCEDURE

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

The "RA" designator (e.g., RA-2, RA-3) identified for each procedure below corresponds to the NIST- identifier for the Risk Assessment control family, as identified in NIST SP 800-53, Revision 5.

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

RA-2 – Security Categorization

For All Systems:

1) Categorize the system and information it processes, stores, and transmits;
2) Document the security categorization results, including supporting rationale, in the security plan for the system; and
3) Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

RA-3 – Risk Assessment

For All Systems and Privacy Control Baseline:

1) Conduct a risk assessment, including:
   a) Identifying threats to and vulnerabilities in the system;
   b) Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits and any related information; and
   c) Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;
2) Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk

assessments;
3) Document risk assessment results in the Risk Assessment Report (RAR) and/or Security Assessment Report (SAR);
4) Review risk assessment results within one (1) week after an assessment, annually thereafter or whenever an update to the risk assessment is made;
5) Disseminate risk assessment results to the SO, ISO, SIO, Information System Security Officer (ISSO), and the Office of Information Security and Privacy (OISP); and
6) Update the risk assessment annually or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

RA-3(1) – Risk Assessment | Supply Chain Risk Assessment

For All Systems:

1) Assess supply chain risks associated with EPA owned or operated systems, system components and system services; and
2) Update the supply chain risk assessment annually, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

RA-5 – Vulnerability Scanning

For All Systems:

1) Monitor and scan for vulnerabilities in the system and hosted applications across all environments (e.g., cloud, on-premise, isolated) to meet the following minimum requirements:
   a) Networked devices[1] every seventy two (72) hours;
   b) Databases monthly;
   c) Internet-facing web applications and web applications associated with an Agency-defined high value asset (HVA), using at a minimum, Dynamic Application Security Testing (DAST) quarterly; and
   d) As required based on management decisions, federal directives, or identified risks and when new vulnerabilities potentially affecting the system are identified and reported;
2) Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
   a) Enumerating platforms, software flaws, and improper configurations;
   b) Formatting checklists and test procedures; and
   c) Measuring vulnerability impact.
3) Analyze vulnerability scan reports and results from vulnerability monitoring;
4) Remediate legitimate vulnerabilities in accordance with the following timelines:
   a) **Critical-** within fifteen (15) calendar days;
   b) **Cybersecurity and Infrastructure Security Agency (CISA)** – **defined Known Exploited Vulnerabilities -** as defined within the catalog;
   c) **High Vulnerabilities** – within thirty (30) calendar days;
   d) **Moderate Vulnerabilities** – within sixty (60) calendar days;

[1] *In accordance with BOD 23-01, networked devices include all IP-addressable assets that can be reached over IPv4 and IPv6 protocols*

e) **Low Vulnerabilities** – ninety (90) calendar days;
f) **Other** – Timelines may be reduced when directed by management, federal mandates (e.g. Binding Operational Directive (BOD), Cybersecurity Coordination, Assessment, and Response (CCAR)), and when threat or risk conditions warrant adjustments; and
g) When vulnerabilities are not remediated within the required timelines a plan of action and milestone (POA&M) must be opened to address remediation plans;

5) Share information obtained from the vulnerability monitoring process and control assessments with ISOs, ISSOs, OISP, and others identified by the system owner to help eliminate similar vulnerabilities in other systems; and
6) Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

RA–5(2) Vulnerability Monitoring and Scanning | Update Vulnerabilities to be Scanned

For All Systems:

1) Update the system vulnerabilities to be scanned no greater than twenty-four (24) hours; prior to a new scan; or when new vulnerabilities are identified and reported.

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

For High Systems:

1) Determine information about the system that is discoverable and take appropriate corrective actions, including notifying the SO or ISO, removing the information, or modifying the system to make the designated information less relevant or attractive to adversaries.

RA–5(5) Vulnerability Monitoring and Scanning | Privileged Access

For Moderate and High Systems:

1) Implement privileged access authorization to all networked devices, applications and databases for all vulnerability scans unless explicit exceptions are approved by the Chief Information Security Officer (CISO) or Chief Information Officer (CIO).

RA–5(11) Vulnerability Monitoring and Scanning | Public Disclosure Program

For All Systems:

1) Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

RA–7 – Risk Response

For All Systems and Privacy Control Baseline:

1) Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

RA–8 – Privacy Impact Assessments

For Privacy Control Baseline:

1) Conduct privacy impact assessments for systems, programs, or other activities before:
   a) Developing or procuring information technology that processes personally identifiable information; and
   b) Initiating a new collection of personally identifiable information that:
      i) Will be processed using information technology; and

ii) Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

RA–9 – Criticality Analysis

For Moderate and High Systems:

1) Identify critical system components and functions by performing a criticality analysis for all EPA FISMA systems at the system design phase and throughout the system lifecycle or whenever there are significant changes to any of the systems' components.

6. ROLES AND RESPONSIBILITIES

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

7. RELATED INFORMATION

- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

8. DEFINITIONS

- **Information** – an instance of an information type.
- **Information Security** – the protection of information and systems from unauthorized access, use, disclosure, disruption, modification or destruction 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, or regulation.

- **Organization** – a federal Agency or, as appropriate, any of its operational elements.
- **Networked devices** – in accordance with BOD 23-01, includes all IP-addressable assets that can be reached over IPv4 and IPv6 protocols.
- **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 a 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 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 a 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 system.
- **Security Categorization** – describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and 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 a 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 a 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 a system.
- **Vulnerability** – weakness in a system, system security procedures, internal controls or implementation that could be exploited.
- **Vulnerability Assessment** – formal description and evaluation of vulnerabilities of a 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.

9. WAIVERS

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

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

10. DIRECTIVE(S) SUPERSEDED

This procedure supersedes Information Directive: CIO-2150-P-14.2, Information Security – Risk Assessment Procedures, April 11, 2016.

11. CONTACTS

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

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2023.12.19 13:38:43 -05'00'

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

APPENDIX A: ACRONYMS & ABBREVIATIONS

BOD	Binding Operational Directive
CCAR	Cybersecurity Coordination, Assessment, and Response
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
DAST	Dynamic Application Security Testing
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HVA	High Value Asset
ISO	Information Security Officer
ISSO	Information System Security Officer
NIST	National Institute of Standards and Technology
OISP	Office of Information Security and Privacy
OMB	Office of Management and Budget
OMS	Office of Mission Support
POA&M	Plan of Action and Milestones
RA	Risk Assessment
RAR	Risk Assessment Report
SAR	Security Assessment Report
SIO	Senior Information Official
SM	Service Mangers
SO	System Owner
SP	Special Publication
U.S.C.	United States Code