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

Information Security – Incident Response (IR) Procedures

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Incident Response (IR) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

2. SCOPE

These procedures address all United States 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. BACKGROUND

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 security requirements by implementing the security controls defined in the NIST SP 800-53, *Revision 5, Security and Privacy Controls for Information Systems and Organizations.*

This document adopts procedures and standards for the EPA consistent with FIPS Publication 200.

5. AUTHORITY

Additional legal foundations for the Incident Response procedure include:

- Federal Information Security Modernization Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)

- OMB Memorandum M-06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,” July 2006
- FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

6. 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 and EPA SO or their official designees and SM for the systems that they oversee.

The "IR” designator (e.g., IR-2, IR-3) identified for each procedure below corresponds to the NIST- identifier for the Incident Response control family, as identified in NIST SP 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations.

NIST defines the applicable IR security and privacy 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.

IR-2 – Incident Response Training

For All Systems:

1) Provide incident response training to system users consistent with assigned roles and responsibilities:
   a) Within thirty (30) days of assuming an incident response role or responsibility or acquiring system access;
   b) When required by system changes; and
   c) Annually thereafter; and
2) Review and update incident response training content annually for system specific functions. Office of Information Security and Privacy (OISP) will review and update the agency-wide information security awareness and privacy training (ISPAT) annually and following a significant security incident, changes to the IR Plan or associated procedures.

IR-2(1) – Incident Response Training I Simulated Events

For High Systems:

1) Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

IR-2(2) – Incident Response Training I Automated Training Environments

For High Systems:

1) Provide an incident response training environment using automated mechanisms.

IR-2(3) – Incident Response Training I Breach

For Privacy Control Baseline:

1) Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

IR-3 – Incident Response Testing

For Moderate and High Systems and Privacy Control Baseline:

1) Test the effectiveness of the incident response capability for the system annually using the following tests: checklists, walk-through, table-top exercises, simulated or live exercises.

IR-3(2) – Incident Response Testing I Coordination with Related Plans

For Moderate and High Systems:

1) Coordinate incident response testing with organizational elements responsible for related plans.

IR-4 – Incident Handling

For All Systems and Privacy Control Baseline:

1) Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;
2) Coordinate incident handling activities with contingency planning activities;
3) Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and
4) Ensure the rigor, intensity, scope and results of incident handling activities are comparable and predictable across the organization.

IR-4(1) – Incident Handling I Automated Incident Handling Processes

For Moderate and High Systems:

1) Support the incident handling process using the following enterprise services: EPA Enterprise IT Service Management System, security information and event management system (SIEM), and EPA Enterprise Security Operations Center automated mechanisms.

IR-4(4) – Incident Handling I Information Correlation

For High Systems:

1) Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

IR-4(11) – Incident Handling | Integrated Incident Response Team

For High Systems:

1) Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in twenty-four (24) hours.

IR-5 – Incident Monitoring

For All Systems:

1) Track and document incidents.

IR-5(1) – Incident Monitoring | Automated Tracking, Data Collection, and Analysis

For High Systems:

1) Track incidents and collect and analyze incident information using the EPA Enterprise IT Service Management System.

IR-6 – Incident Reporting

For All Systems:

1) Require personnel to report suspected incidents to the organizational incident response capability within one (1) hour of identification; and
2) Report incident information to the Computer Security Incident Response Capability (CSIRC) by contacting the Enterprise IT Service Desk (EISD) (sending email to EISD@epa.gov or calling 1-866-411-4-EPA) and the ISO at their respective sites.

IR-6(1) – Incident Reporting | Automated Reporting

For Moderate and High Systems:

1) Report incidents using email to the EISD or other automated mechanisms such as a Security Orchestration and Automation Response (SOAR) tool.

IR-6(3) – Incident Reporting | Coordination with Supply Chain

For Moderate and High Systems:

1) Provide incident information the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

IR-7 – Incident Response Assistance

For All Systems:

1) Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

IR-7(1) – Incident Response Assistance | Automation Support for Availability of Information and Support

For Moderate and High Systems:

1) Increase the availability of incident response information and support using automated mechanisms.

IR-8 – Incident Response Plan

For All Systems:

1) Develop an incident response plan that:
   a) Provides the organization with a roadmap for implementing its incident response capability;
   b) Describes the structure and organization of the incident response capability;
   c) Provides a high-level approach for how the incident response capability fits into the overall organization;
   d) Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   e) Defines reportable incidents;
   f) Provides metrics for measuring the incident response capability within the organization;
   g) Defines the resources and management support needed to effectively maintain and mature an incident response capability;
   h) Addresses the sharing of incident information;
   i) Is reviewed and approved by ISO and SO as appropriate; and
   j) Explicitly designates responsibility for incident response to ISO, ISSO, SA, Database Administrators, Application Owners, SM, external service providers and COOP Coordinators.
2) Distribute copies of the incident response plan to ISSO, SA, Database Administrators, Application Owners, Liaison Privacy Official (LPO), Agency Privacy Official (APO), SM, external service providers and COOP Coordinators;

3) Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;
4) Communicate incident response plan changes to ISSO, SA, Database Administrators, Application Owners, LPO, APO, SM, external service providers and COOP Coordinators; and
5) Protect the incident response plan from unauthorized disclosure and modification.

IR-8(1) – Incident Response Plan | Breaches

For Privacy Control Baseline:

1) Include the following in the Incident Response Plan for breaches involving personally identifiable information:
   a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
   b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
   c) Identification of applicable privacy requirements.

7. 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.

8. RELATED INFORMATION

- NIST Special Publications, 800 Series
- NIST 800-61, Computer Security Incident Handling Guide
- US-CERT Federal Incident Notification Guidelines
- Interim Controlled Unclassified Information Policy, Directive # CIO 2158.0

9. DEFINITIONS

- **Availability** – ensuring timely and reliable access to and use of information.
- **Computer Security Incident Response Capability (CSIRC)** – a capability set up for the purpose of assisting the response to computer security-related incidents; also may be referred to as Computer Incident Response Team (CIRT) or a Computer Incident Response Center (CIRC).
- **Event** – any observable occurrence in an information system and/or network. Examples of events include the system boot sequence, anomalous network traffic, or unusual system processes. Some events may indicate an incident is occurring such

as pre-attack probes or denial-of-service (DoS) attacks. In most cases, events caused by human error, such as unintentionally deleting a critical directory, are the most costly and disruptive.

- **Exercise** – a simulation of an emergency designed to validate the viability of one or more aspects of an IT plan. Exercises are scenario driven. Two common types of exercises are tabletops (discussion based) and functional (operations based). In an exercise, personnel with roles and responsibilities in a particular IT plan meet to validate the content of a plan through discussion of their roles and their responses to emergency situations; execution of responses in a simulated operational environment; or other means of validating responses that does not involve using the actual operational environment.
- **Incident** – an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; the information the system processes, stores or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.
- **Information** – an instance of an information type.
- **Information 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.
- **Malicious Software (Malware)** – software that can be used to compromise computer functions, steal data, bypass access controls or otherwise cause harm to the host computer. Malware is a broad term that refers to a variety of malicious programs.
- **Organization** – a federal agency or, as appropriate, any of its operational elements.
- **Scans (i.e., Network Scan)** – a procedure for identifying active hosts on a network by sending packets to a system to gain information to be used in a subsequent attack or for network security assessment. Internal scanning refers to scans originating from a network that is under the direct control and authority of the EPA; external scanning refers to scans originating from a network that is not under the direct control and authority of the EPA.

- **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).
- **Significant Change** – a change that is likely to substantively affect the security or privacy posture of a system.
- **Test** – an evaluation procedure that uses quantifiable metrics to validate the operability of an IT system or system component in an operational environment specified in an IT plan. A test is conducted in as close to an operational environment as possible; if feasible, an actual test of the components or systems used to conduct daily operations for the organization should be used. The scope of testing can range from individual system components to comprehensive tests of all systems and components that support an IT plan.
- **User** – an individual or (system) process authorized to access an information system.
- **Vulnerability** – a weakness in an information system, system security procedure, security control, or implementation that could be exploited.
- **Written (or in writing)** – a means to officially document the action or decision, either manually or electronically, and includes a signature.

10. WAIVERS

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

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

11. MATERIAL SUPERSEDED

Information Directive: CIO 2150-P-08.2, Information Security – Incident Response Procedures.

12. CONTACTS

For Insert further information, please contact the Office of Mission Support (OMS), Office of Information Security and Privacy (OISP).

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2023.06.20 14:04:23 -04'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information and Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A: ACRONYMS & ABBREVIATIONS

CAT	Category
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CIRC	Computer Incident Response Center
CIRT	Computer Incident Response Team
CSIRC	Computer Security Incident Response Capability
DoS	Denial of Service
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
IDPS	Intrusion Detection and Prevention Systems
IO	Information Owner
IR	Incident Response
ISO	Information Security Officer
ISSO	Information System Security Officer
NIST	National Institute of Standards and Technology
OI	Office of Investigations
OIG	Office of Inspector General
OISP	Office of Information Security and Privacy
OMB	Office of Management and Budget
OTOP	Office of Technology Operations and Planning
PII	Personally Identifiable Information
SLA	Service Level Agreement
SO	System Owner
SP	Special Publication
U.S.C.	United States Code
US-CERT	United States - Computer Emergency Readiness Team