EPA **INFORMATION**
# PROCEDURE

| Information Security – Incident Response Procedures | | | |
|---|---|---|---|
| EPA Classification No.: | CIO 2150-P-08.2 | CIO Approval Date: | 11/30/2015 |
| CIO Transmittal No.: | 16-004 | Review Date: | 11/30/2018 |

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

## INFORMATION SECURITY – INCIDENT RESPONSE PROCEDURES

### 1. PURPOSE

To implement the 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 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 another 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 the 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 the EPA.

### 4. BACKGROUND

Based on federal requirements and mandates, the 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 through the use of the security controls defined in the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. This document addresses the procedures and standards set forth by the EPA, and complies with the family of Incident Response 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) Memorandum M-02-01, “Guidance for Preparing and Submitting Security Plans of Action and Milestones,” October 2001
- OMB Memorandum M-06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,” July 2006
- OMB Memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” May 2007
- OMB Memorandum M-10-28, “Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),” July 2010
- OMB Circular A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal Automated Information Resources,” November 2000
- Homeland Security Presidential Directive (HSPD)-7, “Critical Infrastructure Identification, Prioritization, and Protection,” December 17, 2003
- HSPD-23, “Cyber Security and Monitoring,” January 8, 2008
- Federal Information Processing Standards (FIPS) 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004
- Federal Information Processing Standards (FIPS) 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA Information Security Continuous Monitoring Strategic Plan
- CIO Policy Framework and Numbering System

## 6. PROCEDURES

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

Abbreviations including acronyms are summarized in Appendix A.

### <u>IR-2 – Incident Response Training</u>

**For All Information Systems:**

1) System Owners (SO), in coordination with Information Owners (IO), Information Security Officers (ISO), and Information System Security Officers (ISSO), 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:
    - a) Provide Incident Response (IR) training to information system users that is consistent with their assigned role(s) and responsibility(s). For example, system users may only need to know who to call or how to recognize an incident, while system administrators may need additional training regarding the handling and remediation of incidents. The IR training shall be completed within 60 days of appointment to the role or responsibility.
        - i) Refer to *EPA Information Security – Awareness and Training Procedures* for role-based training requirements.
    - b) Provide additional or supplemental IR training when information system changes occur.
    - c) Include user incident response training regarding the identification and reporting of suspicious activities, both from external and internal sources.
    - d) Maintain a comprehensive record of all IR related training. The electronic log shall include names of participants, information system name(s), type of training, and date of completion. Log entries shall be coordinated with Computer Security Incident Response Capability (CSIRC) and ISOs.
2) The CSIRC, in coordination with SOs, IOs, ISOs, and ISSOs, for EPA-operated systems, shall:
    - a) Assist with training for ISO, ISSO, and end users regarding IR, and CSIRC goals and operations.
        - i) Training may be provided using CSIRC ISO/ISSO Handbook, security newsletters, intranet web pages, briefings, and instructor-led training sessions.
        - ii) All or a sub-set of the end user IR training shall be included in EPA's annual awareness training.
        - iii) Personnel assigned IR roles shall actively participate in role-based IR training and IR plan testing.

iv) IR training should include tabletop exercises or offsite exercises as a part of IR Plan testing.

v) Assist the SO to ensure provided IR training is sufficient in scope and coverage to ensure preparedness for a wide range of IR scenarios.

vi) Use the following NIST SPs as guidance regarding IR training: NIST SP 800-16, *A Role-based Model for Federal Information Technology / Cyber Security Training*, Revision 2; 800-50, *Building an Information Technology Security Awareness and Training Program*; 800-61, *Computer Security Incident Handling Guide*, Revision 2; and 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*.

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

**For High Information Systems:**

1) SOs, in coordination with, CSIRC, IOs, ISOs, and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs and the CSIRC, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Provide for simulated events to be incorporated into incident response training to facilitate the effective responses by personnel in crisis situations.

      i) Tailor simulated events to suit user roles and responsibilities.

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

**For High Information Systems:**

1) SOs, in coordination with the CSIRC, IOs, ISOs, and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with IOs and the CSIRC, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Provide automated training environments for training all systems users regarding a range of information security threats.

      i) Training environments shall consist of automated mechanisms such as an automatic alert system, which simulate a live threat environment.

      ii) Automated mechanisms shall be thorough in scope, realistic and tailored to fit specific user roles and responsibilities.

### IR-3 – Incident Response Testing

**For Moderate and High Information Systems:**

1) SOs, in coordination with ISOs, IMOs, IOs, ISSOs, Common Control Providers (CCP) and Security Control Assessors (SCA), for EPA-operated systems, shall; and SMs, in coordination with the CISRC, IOs, ISOs, IMOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Test or exercise the IR capability for all information systems annually, and review checklists quarterly to ensure all personnel are prepared to react to emergencies.

i) Testing shall include scenario-based exercises to determine the ability of the Agency to respond to information security incidents.

ii) At a minimum, tabletop exercises shall be performed. However, functional exercises that are more robust are recommended, such as simulations and/or comprehensive exercises.

b) Document the results of incident response tests/exercises within the Incident Response (IR) Plan. The plan and test/exercise results shall be reviewed annually.

c) Develop, review, and update agency-level IR Test Plans, and update incident response plans annually.

d) Identify and remediate IR Plan weaknesses using the results of incident response tests/exercises.

e) Address corrective actions in the Plan of Action and Milestones (POA&M) for the particular information system.

f) Use NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities,* and NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, as guidance regarding test, training, and exercise programs for information technology plans and capabilities.

### IR-3 (1) – Incident Response Testing I Automated Testing

Not selected as part of the control baseline.

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

**For Moderate and High Information Systems:**

1) SOs, in coordination with CSIRC, CCPs, ISOs, IMOs, and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with the CSIRC, IOs, IMOs, ISSOs, CCPs, and SCAs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Coordinate IR testing throughout their respective organizations; to include organizational elements responsible for related plans. The following documents may be required for testing and documentation during testing:

i) Business Continuity Plans,

ii) Contingency Plans,

iii) Disaster Recovery Plans,

iv) Continuity of Operations Plans, and

v) Occupant Emergency Plans.

## IR-4 – Incident Handling

**For All Information Systems:**

1) The CSIRC, in coordination with SOs, ISOs, ISSOs, and IOs, for EPA-operated systems, shall; and SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Provide an organizational incident handling capability for security incidents that incorporates incident response preparation, detection, analysis, containment, eradication, and recovery.

      **Note:** Malicious software (Malware) incidents often require special handling techniques. See Appendix B: *Malware Handling* for the containment, isolation, and eradication of Malware and recovery from Malware-related incidents.

      **Note**: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events.

   b) Create a process that coordinates incident handling and contingency planning activities.

   c) Incorporate 'lessons learned' information from past and present incident-handling response procedures, training, and test/exercises, and implement the results accordingly.

   d) Provide for the protection of EPA's information assets by personnel who can respond to, mitigate, and resolve actual and potential incidents and events by defining response requirements for Agency reporting and response to information security incidents.

   e) Provide a Service Level Agreement (SLA) for agency response to advisories that are received from external Computer Emergency Response Team (CERT) organizations that may have a potential impact on Agency information systems.

   f) Promote awareness of information security risks so the Agency is better prepared to handle those incidents and is better protected against them.

   g) Respond to a reported incident according to defined response requirements.

   h) Provide management and logistical support to system administrators for timely reporting, tracking, resolving, and documenting detected information security incidents. Coordinate with the Office of Technology Operations and Planning (OTOP) security staff as needed for logistical support.

   i) Develop, publish, and maintain operational procedures required for ISO/ISSO site-specific handling of information security incidents.

   j) Receive and forward all appropriate incident and vulnerability notifications (e.g., CERT) to the IO, SO, and ISSO for respective systems affected by the incident or vulnerability.

   k) Maintain a telephone contact list of System Administrators (SA), SM, and ISO to enable notification and coordination according to defined response requirements.

l) Establish and maintain notification and escalation procedures for reporting and responding to information security incidents at the site according to defined response requirements.

2) SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Coordinate IR activities with EPA internal organizational units, and external organizations, such as:

      i) Office of Inspector General (OIG) – Office of Investigations (OI)

      ii) Office of Public Affairs (OPA)

      iii) Human Resources

      iv) Facility Security

      v) Congressional Affairs

      vi) Office of General Counsel (OGC)

   b) Require that all personnel directly involved with incident handling sign a Non-Disclosure Agreement (NDA).

   c) Discuss Incident details only on a need-to-know basis with authorized personnel.

   d) Assist in tracking, resolving, and documenting reported information security incidents, per CSIRC-established SLAs and procedures.

   e) Utilize the following for guidance regarding incident handling:

      i) NIST SP 800-36, *Guide to Selecting Information Technology Security Products*;

      ii) NIST SP 800-61, *Computer Security Incident Handling Guide*, Revision 2;

      iii) NIST SP 800-83, *Guide to Malware Prevention and Incident Handling for Desktops and Laptops*, Revision 1;

      iv) NIST SP 800-86, *Guide for Integrating Forensic Techniques into Incident Response*;

      v) NIST SP 800-92, *Guide to Information Security Log Management*;

      vi) NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*;

      vii) NIST SP 800-101, *Guidelines on Mobile Device Forensics*, Revision 1; and

      viii) Other appropriate guidance, as necessary.

   f) Activate and implement a security incident handling capability during all stages of the NIST incident response life cycle (See Figure 1), including:

      i) Preparation

      ii) Detection and Analysis

      iii) Containment, Eradication, and Recovery

      iv) Post-Incident Activities

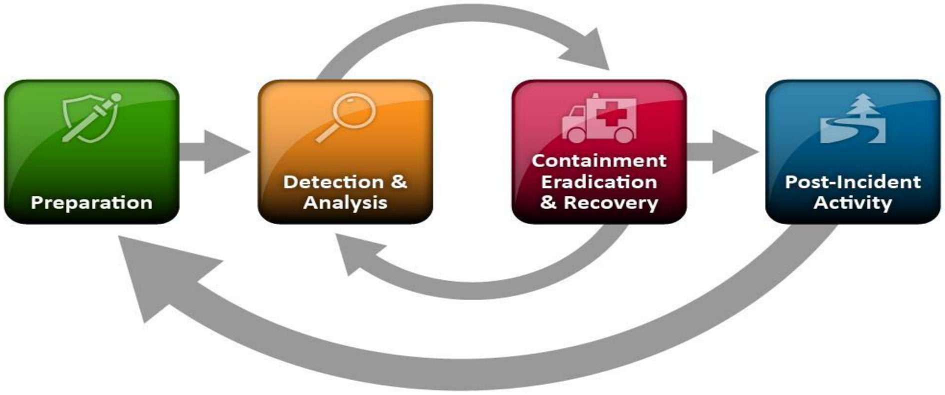

**Figure 1 - Incident Response Life Cycle**

**For FedRAMP[1] Low and Moderate Information Systems:**

1) SMs, in coordination with SOs, the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Require that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

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

**For Moderate And High Information Systems:**

1) The CSIRC, in coordination with SOs, IOs, ISOs, and ISSOs, for EPA-operated systems, shall; and SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Employ automated mechanisms (e.g., online incident management systems) to support the Agency's incident handling process.
   b) Implement a process that facilitates the sharing of various reporting procedures and dissemination of incident information.

### IR-4 (2) Incident Handling I Dynamic Reconfiguration

Not selected as part of the control baseline.

### IR-4 (3) Incident Handling I Continuity of Operations

Not selected as part of the control baseline.

[1] *The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.*

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

**For High Information Systems**

1) The CSIRC, in coordination with SOs, ISOs, ISSOs, and IOs, for EPA-operated systems, shall; and SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Enact automated processes for the purpose of correlating security event and incident information.
   b) Create processes to provide information for the enhancement of organizational and Agency information security awareness programs and incident response programs.

### IR-4 (5) Incident Handling I Automatic Disabling of Information System

Not selected as part of the control baseline.

### IR-4 (6) Incident Handling I Insider Threats – Specific Capabilities

Not selected as part of the control baseline.

### IR-4 (7) Incident Handling I Insider Threats – Intra-organization Coordination

Not selected as part of the control baseline.

### IR-4 (8) Incident Handling I Correlation with External Organizations

Not selected as part of the control baseline.

### IR-4 (9) Incident Handling I Dynamic Response Capability

Not selected as part of the control baseline.

### IR-4 (10) Incident Handling I Supply Chain Coordination

Not selected as part of the control baseline.

### IR-5 – Incident Monitoring

**For All Information Systems:**

1) The CSIRC, in coordination with SOs, ISOs, ISSOs, and IOs, for EPA-operated systems, shall; and SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Track and document Information system security incidents using automated and manual systems and methods.

      **Note*:*** Documenting information system security incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling.

Incident information can be obtained from a variety of sources, including incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

b) Log all incidents electronically that involve EPA systems and data.

i) The logs shall be maintained at the designated official repository and at the site of the incident where on-site response teams report and take actions related to incidents.

ii) Logs shall be maintained in accordance with EPA Records Schedule 1012.

iii) Logs pertaining to a law enforcement action may subject them to retention requirements that are in accordance with EPA Records Schedule 698.

2) The CSIRC, in coordination with SOs, IOs, ISOs, and ISSOs, for EPA-operated systems, shall:

a) Use EPA's Remedy system (or equivalent) as the Agency repository for tracking incidents reported through the EPA Call Center (EPA CC).

i) The security incident component shall be separate from other tracking data to ensure only authorized personnel have access to the security incident information.

b) Use the workflow capabilities of EPA's Remedy system (or equivalent) to request incident response assistance from the ISO and ISSO.

i) The OIG-OI shall have access to the Agency's incident tracking database(s) for actual and potential criminal investigative actions.

ii) NIST SP 800-61, *Computer Security Incident Handling Guide*, Revision 2 shall be utilized as guidance on monitoring incidents.

### IR-5 (1) Incident Monitoring | Automated Tracking / Data Collection

**For High Information Systems:**

1) The CSIRC, in coordination with SOs and IOs, for EPA-operated systems, shall; and SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Employ automated mechanisms to assist in the tracking of security incidents.

i) Automated mechanisms may also assist in the collection and analysis of information regarding security incidents.

**Note*:*** Automated mechanisms for tracking security incidents and collecting/analyzing incident information include the Einstein network-monitoring device and monitoring online CIRCs, or other electronic databases of incidents.

## IR-6 – Incident Reporting

**For All Information Systems:**

**Note**: The intent of this control is to address specific incident reporting requirements within an organization, and the formal incident reporting requirements for federal agencies and their subordinate organizations.

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Report security incident information to the CSIRC and designated IR personnel at their respective sites.
   b) Ensure the type of security incident reported, the content and timeliness of the reports, and the list of designated reporting authorities is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
   c) Report incidents within the timeframe indicated by the incident category, (CAT 0 – CAT 4). See Appendix C: *US-CERT and EPA Incident Categories and Reporting Timeframes* for incident categories and mandatory reporting timeframes.
   d) Submit incident reports per the requirements in *Appendix B* even if the report is incomplete.
   e) Ensure Agency managers and supervisors follow reporting guidelines when reporting incident information to designated incident response representatives.
   f) Report all known or suspected information security incidents or vulnerabilities immediately using the following reporting guidelines:
      i) The preferred order of notification is:
         (1) Personnel shall notify the ISO immediately. If the ISO is not immediately available, personnel shall immediately contact the EPA CC directly.
         (2) The ISO shall notify the EPA CC, who in turn shall contact CSIRC.
      ii) During normal duty hours, EPA CC shall:
         (1) Open a Problem Management Record (PMR) for each reported incident.
         (2) Route the PMR to the CSIRC Coordinator.
         (3) Forward all security-related calls to CSIRC.
      iii) Outside of normal duty hours, EPA CC shall:
         (1) Maintain a Voice Response Unit (VRU) capability for after-hours reporting of information security incidents.
         (2) Automatically relay calls to the 24x7 network operations personnel who shall contact the on-call CSIRC staff member.

         **Note:** Once incident information is reported to CSIRC, the CSIRC team shall conduct an initial inquiry to verify whether an incident actually occurred and provide immediate mitigation, if possible. The CSIRC shall record incident information in a tracking system, validate the incident, determine the magnitude of the incident, and determine further actions.

2) The CSIRC, in coordination with SOs, IOs, ISOs, and ISSOs, for EPA-operated systems, shall:

   a) Report incidents to US-CERT, the OIG, Office of Public Affairs, the EPA Physical Security Officer, and EPA Senior Management (e.g., Deputy Administrator, Chief Information Officer [CIO]), as appropriate, for the incident and established reporting requirements in *Appendix B*.

   **Note*:*** Current federal policy requires that all federal agencies report security incidents to the US-CERT within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling, unless specifically exempted from such requirements.

   b) Contact the OIG-OI whenever there is a possibility of information system related criminal activity.

      i) The OIG shall serve as the primary point of contact for coordination with law enforcement agencies in regards to incident reporting. Any contact with law enforcement agencies shall be coordinated through the OIG.

      ii) All criminal-related information provided to outside agencies other than law enforcement shall be reviewed by EPA's OGC.

   c) Inform other system personnel about incidents that may affect them, in accordance with response actions and escalation protocols established for incidents.

   d) Create and disseminate information security incident reports.

      i) This activity may require interfacing with the ISO, ISSO and US-CERT.

   e) Coordinate, when necessary, with the Federal Bureau of Investigation (FBI), US Cert, and EPA's Office of Homeland Security.

   f) Refrain from releasing security-related incident information to any external entity, other than reporting to US-CERT, unless approved by the Senior Agency Information Security Officer (SAISO).

      i) Incident reports to external entities shall be also approved by the SAISO prior to the release.

      ii) All information provided to outside agencies shall be reviewed by EPA's OGC.

      iii) All requests for information related to CSIRC activities shall be forwarded to EPA's OPA, as approval by the SAISO. Information shall not be disseminated directly to the media without approval from the SAISO.

      iv) CSIRC personnel shall not discuss any portion of an incident with anyone outside CSIRC reporting channels without the express approval of the SAISO. All information derived from working with CSIRC shall be considered sensitive and the property of the Agency.

   g) Submit periodic summary incident reports to individuals designated by the SAISO.

h) Provide other periodic information security reports to US-CERT as appropriate for the incident and established reporting requirements in *Appendix B*.

i) Provide consolidated monthly incident reports to the SAISO. The monthly incident reports shall include, to the extent possible, the following elements regarding the detected network activity:

   i) Incident date and time, including time zone

   ii) Indication of scan, probe, or attempted access

   iii) Source IP, port, and protocol

   iv) Destination IP, port, and protocol

   v) Operating System, including version, patches, etc.

   vi) System function (e.g., Domain Name Server [DNS], web server, workstation)

   vii) Antivirus software installed, including version, and latest updates

   viii) Physical location of the system(s) involved in the incident (e.g., Washington, DC)

   ix) Method used to identify the incident (e.g., IDS, audit log analysis, system administrator)

   x) Impact to Agency

   xi) Resolution actions

3) ISOs and ISSOs, in coordination with SOs and IOs, for EPA-operated systems, shall:

   a) Forward their monthly collection of incident information to the CSIRC.

4) All Agency personnel shall ensure service providers:

   a) Adhere to NIST SP 800-61, *Computer Security Incident Handling Guide*, Revision 2 regarding incident reporting for EPA-operated systems and all systems operated on behalf of the EPA.

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

**For Moderate and High Information Systems:**

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Employ automated mechanisms to assist in reporting security incidents.

### IR-6 (2) Incident Reporting | Vulnerabilities Related to Incidents

Not selected as part of the control baseline.

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

Not selected as part of the control baseline.

### IR-7 – Incident Response Assistance

**For All Information Systems:**

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with the CSIRC and IOs for systems operated on behalf of the EPA, shall ensure service providers:
   a) Provide access to appropriate organizational IR resources for the handling and reporting of information security incidents.

      **Note:** These resources may include access to forensic services, web-based support, and EPA incident response capability. CSIRC serves as the EPA's incident response support resource and offers assistance and advice to users regarding potential incidents and the incident handing and reporting procedures.

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

**For Moderate and High Information Systems:**

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Employ automated mechanisms to increase availability of incident response information and support.

      **Note**: Examples of automated mechanisms include automated answering and/or ticketing system for help desk, Really Simple Syndication (RSS) and Atom feeds, subscriptions, distribution lists, agency supported social networks, etc. Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increased response capabilities and support.

### IR-7 (2) Incident Response Assistance | Coordination with External Providers

**For FedRAMP Moderate Information Systems:**

1) SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Create an incident response capability, per FedRAMP requirements, and identify incident response team members to the EPA and other external incident response providers with related organizational goals and connected systems.
      i) Communicate to the EPA, including CSIRC, incident response team members so EPA can provide incident response assistance and coordination with the service providers in the event of an incident.
   b) Establish and maintain a cooperative relationship between its IR capability and the EPA's IR capability, and other external, key providers of information systems

protection, as warranted for the protection of the information system and the information therein.

## IR-8 – Incident Response Plan

**For All Information Systems:**

1) SOs, in coordination with IOs, for EPA-operated systems, shall; and SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Develop an IR Plan that:
      i) Provides the organization with a roadmap for implementing its incident response capability;
      ii) Describes the structure and organization of the incident response capability;
      iii) Provides a high-level description of how the incident response capability fits into the overall organization;
      iv) Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
      v) Defines reportable incidents.
      vi) Provides metrics for measuring the incident response capability within the organization;
      vii) Defines the resources and management support needed to effectively maintain and mature an incident response capability.
      viii) Is reviewed and approved by organizational information security representatives, senior leadership, and the applicable Incident Response Team Lead / Official.
   b) Distribute copies of the IR Plan to organizational senior leadership, information security personnel, and personnel possessing significant incident response responsibilities.
   c) Review the IR Plan annually.
   d) Update and revise the IR Plan to address system/organizational changes or problems encountered during plan implementation, execution or testing.
   e) Communicate IR Plan changes to organizational senior leadership, information security personnel, and personnel possessing significant incident response responsibilities.

      **Note:** It is important that organizations have a formal, focused, and coordinated approach to incident response. The organization’s mission, strategies, and goals for incident response help determine the structure of its incident response capability.

## IR-9 – Information Spillage Response

**For FedRAMP Moderate Information Systems:**

1) SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Respond to information spills by quickly identifying the information involved in the contamination.

b) Assign specific personnel with responsibilities of identifying and handling information spills.

c) Eradicate the spilled information from the contaminated information system(s) or component(s).

d) Provide information spillage response training to all designated incident spillage response personnel.

e) Implements procedures to ensure that personnel are able to carry out their assigned tasks while affected systems are undergoing corrective measures.

f) Employ safeguards to ensure that personnel who are inadvertently exposed to information not within their security access authorization protect the information from unauthorized exposure.

### IR-9 (1) – Information Spillage Response | Responsible Personnel

**For FedRAMP Moderate Information Systems:**

1) SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Assign an information security representative with the responsibility of responding to information spills.

### IR-9 (2) – Information Spillage Response | Training

**For FedRAMP Moderate Information Systems:**

1) SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Provide training to personnel regarding the proper response to information spills on an annual basis, at a minimum.

### IR-9(3) – Information Spillage Response | Post-Spill Operations

**For FedRAMP Moderate Information Systems:**

1) SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Implement controls to ensure that personnel affected by an information spill are able to carry out essential functions while contaminated systems are undergoing corrective actions.

### IR-9(4) – Information Spillage Response | Exposure to Unauthorized Personnel

**For FedRAMP Moderate Information Systems:**

1) SMs, in coordination with the CSIRC and IOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Employ security safeguards for personnel exposed to information spills not within their assigned authorization to access.

### IR-10 – Integrated Information Security Analysis Team

Not selected as part of the control baseline.

## 7. RELATED DOCUMENTS

- NIST Special Publications, 800 Series
- The National Strategy to Secure Cyberspace, February 2003 - www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

## 8. ROLES AND RESPONSIBILITIES

### Chief Information Officer (CIO)

1) The CIO has the following responsibilities with respect to incident response:
   a) Develop, implement, and maintain capabilities for detecting, reporting, and responding to information security incidents.

### Common Control Providers (CCP)

1) CCPs have the following responsibilities with respect to incident response:
   a) Develop and manage plans of actions and milestones for discovered weaknesses.
   b) Conduct impact analyses for proposed or actual changes to systems or their operational environments.
   c) Coordinate with the SAISO in responding to information security data calls, audit requests, and reporting.
   d) Coordinate with the CIO, Risk Executive, Risk Executive Group, SAISO and others involved with securing Agency information and systems to ensure risks are managed to an acceptable level.

### Computer Security Incident Response Capability (CSIRC)

1) CSIRC has the following responsibilities with respect to incident response:
   a) Protect the Agency’s information assets and network.
   b) Work in conjunction with supporting entities to establish tools and resources in anticipation of security incidents and events.
   c) Work with the information security community to make recommendations for securing networks, systems, and applications.
   d) Educate ISOs and end users on CSIRC goals and operations.

e) Define the process by which the Agency responds to computer security-related incidents such as computer viruses, unauthorized user activity, and serious software vulnerabilities.

f) Provide a service level for Agency response to computer security incident reporting.

g) Provide a service level for Agency response to advisories that are received from external organizations and that may have a potential impact on Agency computer systems.

h) Provide a method to promote computer security risk awareness so the Agency is better prepared to handle incidents and is protected against them.

i) Take actions to verify that an incident actually occurred upon learning of a potential incident.

j) Determine the scope and impact of each intrusion and prioritize actions accordingly.

k) Determine the magnitude of the incident once an incident is validated.

l) Maintain an electronic log of and track all incidents that occur at the EPA.

m) Provide scripts to the EPA CC to ensure that potential security events are properly identified, sufficient initial information is obtained for follow-up and Remedy tickets are properly routed.

n) Ensure that Remedy tickets for actual and potential incidents are:

   i) Updated throughout the incident management life cycle, and

   ii) Made available only to appropriate personnel.

o) Report and coordinate incidents with US-CERT, OIG, OPA, the EPA Physical Security Officer, and EPA Senior Management (e.g., CTO, SAISO), as appropriate.

p) Provide information security reports and updates to US-CERT periodically.

q) Provide an incident support resource that offers assistance and advice to users regarding potential incidents, vulnerabilities, and the incident handling/reporting procedures.

r) Manage and coordinate all incident responses to malicious software intrusions.

s) Assist the SAISO in establishing efficient and effective Line of Business Center reporting and non-duplication related to incidents involving EPA information resources.

t) Utilize post-incident analysis to determine if and when additional alerts should be issued to users specifying actions to reduce vulnerabilities exploited during incidents.

u) Assess impacts on the EPA's security posture and controls as a result of handling and resolving incidents.

v) Provide lessons learned for SO, ISO, ISSO, senior managers, and others with recommendations to mitigate weaknesses identified during analysis.

w) Determine specific response actions and escalation protocols for each incident.

**CSIRC Operations Manager**

1) The CSIRC Operations Manager has the following responsibilities with respect to incident response:

a) Provide management or technical direction, as appropriate, to contracted CSIRC capabilities.

b) Facilitate annual incident response training for the CSIRC and IT security community supported by the EPA's IR Plan.

c) Maintain a comprehensive electronic log of all information security IR Plan related training.

d) Interface with the ISO, US-CERT, OIG-IO, and other law enforcement, as necessary.

e) Define the timeliness of each step within the information security incident response reporting process.

**Note:** The total time allocated to all steps shall not exceed the total time in OMB Memo M-06-16, including requirement to report the loss of PII in one hour.

f) Provides weekly incident reports to the SAISO and incident reports to US-CERT, as required.

**EPA Call Center (CC)**

1) The EPA CC has the following responsibilities with respect to incident response:

a) Serve as the central point of contact for receiving reports of computer security incidents.

b) Serve as a PMR for each reported incident.

c) Route the PMR to the CSIRC for resolution in accordance with procedures established in this document.

d) Maintain the OTOP VRU capability for after-hours reporting of computer security incidents.

**Information Owner (IO)**

1) The IO has the following responsibilities with respect to incident response:

a) Coordinate with the System Owner in providing IR training to information system users that is consistent with their assigned role(s) and responsibility(s).

b) Coordinate with CSIRC.

**Information Security Officer (ISO)**

1) The ISO has the following responsibilities with respect to incident response:

a) Report detected scans, probes, and attempted accesses that are either internal to an EPA network or external to and directed at an EPA network.

b) Respond immediately to a reported incident.

c) Provide management and logistical support to system administrators for timely reporting, tracking, resolving, and documenting detected computer security incidents.

d) Coordinate with CSIRC and IT management to resolve and close outstanding incidents within SLA timeframes established by CSIRC.

e) Coordinate with the OTOP security staff and CSIRC as needed for technical support and direction required to provide management and logistical support to system administrators and to document the incident.

f) Collect information from the SO on items such as the level of access an intruder gained and how the intruder was able to breach defenses.

g) Receive and forward all CSIRC notifications to individuals responsible for affected systems and inform users of vulnerabilities or threats as appropriate.

**Information System Security Officer (ISSO)**

1) The ISSO has the following responsibilities with respect to incident response:

a) Support the ISO in accomplishing ISO responsibilities for assigned systems.

b) Maintain up-to-date contact information of SO, site system administrators, system managers, and other security personnel.  Provide the contact information to CSIRC and update as needed.

**National Computer Center (NCC)**

1) NCC has the following responsibilities with respect to incident response:

a) Affirm or modify the emergency actions taken and notify OTOP and Office of Environmental Information (OEI) management.

b) Direct immediate technical measures, as well as subsequent repair and resolution. Any communication necessary with the administrators and ISO communities shall be the responsibility of NCC.

c) Enforce the requirement for oversight and diligence in intrusion detection to include eight additional hours of near real-time sensor monitoring.

d) Provide access to network and security applications, devices, and appliances when requested by CSIRC.

e) Identify, document and maintain a database that includes all categorizations, IO, SO and ISSO actions for respective systems affected by the incident or vulnerability and applicable systems hosted by NCC.

**Office of Enforcement and Compliance Assistance (OECA), National Enforcement Investigations Center (NEIC)**

1) OECA-NEIC has the following responsibilities with respect to incident response:

a) Assist CSIRC and ISO in forensic capabilities, when possible and needed.

**Office of Inspector General (OIG), Office of Investigations (OI)**

1) OIG-OI has the following responsibilities with respect to incident response:

a) Determine if an incident identified by CSIRC as possibly criminal in nature is actually criminal in nature.

b) Serve as the primary point of contact for coordination with law enforcement.

c) Conduct criminal investigations of incidents when criminality is determined.

d) Assist CSIRC and ISO in forensic capabilities, when possible and needed.

**Office of General Counsel (OGC)**

1) OGC has the following responsibilities with respect to incident response:
    a) Review incident reports to be provided to external entities for criminal-related incidents.

**Office of Public Affairs (OPA)**

1) OPA has the following responsibilities with respect to incident response:
    a) Disseminate to the media information relating to incident handling that has been approved by the SAISO.

**Personal Computer Site Coordinator (PCSC)**

1) The PCSC has the following responsibilities with respect to incident response:
    a) Make initial determinations regarding problems with personal computer (PC) hardware and software in conjunction with PC customers.

**Security Control Assessor (SCA)**

1) The SCA has the following responsibilities with respect to incident response:
    a) Identify weaknesses or deficiencies in EPA information systems related to security control design, implementation, and maintenance. Senior Agency Information Security Officer (SAISO).
    b) Provide a Security Assessment Report (SAR) to SOs, IOs, SMs, ISOs, and ISSOs that accurately reflects the status of security controls that have been assessed.

**Security Agency Information Security Officer (SAISO)**

1) The SAISO has the following responsibilities with respect to incident response:
    a) Ensure the CIO is informed of security incidents.
    b) Ensure the organization has adequate procedures for information security incident handling.
    c) Ensure the agency information security program adequately addresses incident handling responsibilities and procedures within the organization.
    d) Coordinate with the OTOP Director to ensure the Agency can adequately detect, respond, and report information security incidents.
    e) Coordinate evaluation and resolution of CSIRC mitigation recommendations.
    f) Coordinate with the Privacy Office, and ensure privacy policies and procedures are followed when an incident involves PII.
    g) Approve security-related incident information for release to any external entity, other than reports to US-CERT, FBI, or the intelligence community.
    h) Develop, maintain, and publish procedures required for site-specific handling of computer security incidents as needed.
    i) Provide oversight of CSIRC, including oversight of incident management.

j) Ensure a current telephone contact list of site system administrators, system managers, and ISOs is maintained.

k) Ensure that the EPA IR Test Plan is reviewed and updated annually.

l) Ensure that all incidents involving PII are reported to US-CERT within 1 hour after a potential or known incident is reported.

m) Review and approve any computer security incident-related information prior to permitting it to be released to an external entity.

n) Ensure agreements with Line of Business providers to implement effective, efficient, and non-duplicative incident reporting that is accurately reflective of EPA information-related incidents.

o) Ensure computer security incidents are properly reported.

p) Develop, distribute, review, and revise an IR Plan.

q) Ensure Senior Management (e.g., OTOP Director) is informed of incidents and incident status in a timely manner.

r) Coordinate with the Privacy Office and ensure privacy policies and procedures are followed when an incident involves PII.

**Service Manager (SM)**

1) Service Managers have the following responsibilities with respect to incident response:

a) Provide IR training to information system users and service providers, in coordination with SOs and IOs that is consistent with their assigned role(s) and responsibility(s).

b) Decide who has access to the service (and with what types of privileges or access rights) and ensure service users and support personnel receive the requisite security training (e.g., instruction in rules of behavior).

c) Ensure terms of service and other contractual agreements satisfy the security and privacy requirements applicable to EPA information systems and information.

**System Administrator (SA)**

1) System administrators have the following responsibilities with respect to incident response:

a) Scan the information system(s) for actual data/document(s) and the presence of moderate and/or high sensitivity or PII information.

b) Scan network elements (e.g., email servers, content cache servers, etc.) for possible unauthorized disclosure and/or distribution and the presence of moderate and/or high sensitivity or PII information.

c) Evaluate the existence of interconnected information systems for additional possible unauthorized disclosure and/or distribution in partner networks.

d) Analyze the email server logs to identify other contaminated systems when email is involved in an incident.

e) Analyze server audit logs to help identify recipients of downloaded files when HTTP and FTP are involved.

f) Assume that storage devices accessed and backups conducted during the time of the incident are contaminated and require containment.

g) Isolate contaminated components from the network.

h) Determine the severity of the unauthorized disclosure and/or distribution if the network has been contaminated.

i) Make a copy of the contaminated file.

j) Collect all backup tapes, CD-ROMs, and/or disks of the contaminated systems.

**System Owner (SO)**

1) System Owners have the following responsibilities with respect to incident response:

   a) Implement policies, procedures, and control techniques identified in the Agency information security program.

   b) Coordinate with the CSIRC.

   c) Collect information from the SO on items such as the level of access an intruder gained and how the intruder was able to breach defenses.

   d) Provide IR training to information system users that is consistent with their assigned role(s) and responsibility(s).

   e) Maintain a comprehensive record of all IR related training.

## 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).
- *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* – individual or (system) process authorized to access an information system.
- *Vulnerability* – weakness in an information system, system security procedure, security control, or implementation that could be exploited.
- *Written* (or in writing) – means 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 Director, OTOP shall coordinate to maintain central repository of all waivers.

## 11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

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

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

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

## 12. MATERIAL SUPERSEDED

- EPA Information Security – Interim Incident Response Procedures, Version 2150-P-08.1, July 19, 2012

## 13. ADDITIONAL INFORMATION

EPA’s Computer Security Incident Response Capability (CSIRC) – http://cfint.rtpnc.epa.gov/otop/security/csirc/csirc_home.cfm

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

## *APPENDIX A: ACRONYMS & ABBREVIATIONS*

| | |
|---|---|
| CAT | Category |
| CC | Call Center |
| CCP | Common Controls Provider |
| CD-ROM | Compact Disc Read-Only Memory |
| CERT | Computer Emergency Response Team |
| CIO | Chief Information Officer |
| CIRC | Computer Incident Response Center |
| CIRT | Computer Incident Response Team |
| COOP | Continuity of Operations Plan |
| CSIRC | Computer Security Incident Response Capability |
| CTO | Chief Technology Officer |
| DHS | Department of Homeland Security |
| DNS | Domain Name System |
| DoS | Denial of Service |
| EPA | Environmental Protection Agency |
| FBI | Federal Bureau of Investigation |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act |
| FTP | File Transfer Protocol |
| HSPD | Homeland Security Presidential Directive |
| HTTP | Hypertext Transfer Protocol |
| IDS | Intrusion Detection System |
| IP | Internet Protocol |
| IO | Information Owner |
| IR | Incident Response |
| ISO | Information Security Officer |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| LAN | Local Area Network |
| NCC | National Computer Center |
| NEIC | National Enforcement Investigations Center |
| NIST | National Institute of Standards and Technology |
| NSOC | Network Security Operations Center |
| OECA | Office of Enforcement and Compliance Assistance |
| OEI | Office of Environmental Information |
| OI | Office of Investigations |
| OIG | Office of Inspector General |
| OGC | Office of General Counsel |
| OMB | Office of Management and Budget |
| OPA | Office of Public Affairs |
| OSCAR | Operational Status Categories during Alerts and Risks |
| OTOP | Office of Technology Operations and Planning |
| PC | Personal Computer |
| PCSC | Personal Computer Site Coordinator |
| PII | Personally Identifiable Information |
| PMR | Problem Management Record |
| POA&M | Plan of Action and Milestones |
| RSS | Really Simple Syndication |
| SA | System Administrator |

| | |
|---|---|
| SAISO | Senior Agency Information Security Officer |
| SCA | Security Controls Assessor |
| SIO | Senior Information Official |
| SLA | Service Level Agreement |
| SM | Service Manager |
| SO | System Owner |
| SP | Special Publication |
| USC | United States Code |
| US-CERT | United States - Computer Emergency Readiness Team |
| VRU | Voice Response Unit |
| WAN | Wide Area Network |

## APPENDIX B: MALWARE HANDLING

***[Containment and Isolation Actions]***

**For All Information Systems:**

1) The SAISO, in coordination with SOs and IOs for EPA-operated systems; and IOs, in coordination with SMs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Institute measures to stop and contain the spread of malware, and/or isolate affected systems.
   b) Enact pre-established controls to ensure priority handling of suspicious system events.
   c) Provide clear instructions to users regarding the containment of malware known to exist on the network following detection of the malware within organizational systems.
   d) Enact an organizational incident handling capability for malware-related security incidents that incorporates clear steps for incident response preparation, detection, analysis, containment, eradication, and recovery.
   e) Provide a process to coordinate incident-handling activities, and incorporate lessons-learned information from past incidents, training, and test/exercises.
   f) Eliminate or disable services that may be used by the malware as a means to propagate throughout a system or network of systems and provide clear user instructions to prevent system administrators and users from performing actions that may inadvertently assist to propagate malware across systems and networks.
   g) Offer specialized training to personnel designated to handle malware incidents and institute measures that facilitate and promote effective malware response, containment and resolution, such as:
      i) Providing malware incident trained and response-capable personnel that are available during normal business hours and on call during the off-hours.
      ii) Creating and maintaining a service level agreement (SLA) for agency response to advisories that are received from external organizations (e.g., Computer Emergency Response Team (CERT) organizations) that may have a potential impact on Agency information systems.
      iii) Promoting awareness of information security risks so the Agency is better prepared to handle those incidents and is better protected against them.
      iv) Responding to malware incidents according to pre-defined response requirements.
      v) As required, coordinating with the Office of Technology Operations and Planning (OTOP) security staff as needed for logistical support.
      vi) Developing, maintaining and publishing operational procedures required for ISO/ISSO site-specific handling of malware incidents.
      vii) Receiving and forwarding malware and vulnerability notifications to appropriate Information Owners (IOs), System Owners (SOs), and ISSOs for affected systems.
      viii) Maintaining a contact list of system administrators, system managers, and ISOs to enable notification and coordination according to response requirements.
      ix) Establishing and maintaining notification and escalation procedures for malware incidents at the site, according to defined response requirements.
      x) Using the following NIST SPs for guidance for malware and malware incident handling: 800-36, *Guide to Selecting Information Technology Security Products*;

800-61*, Computer Security Incident Handling Guide*, Revision 2; 800-83, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, Revision 1; 800-86, *Guide to Integrating Forensic Techniques into Incident Response*; 800-92, *Guide to Computer Security Log Management*; 800-94, DRAFT *Guide to Intrusion Detection and Prevention Systems* (IDPS), Revision 1; and 800- 101, *Guidelines on Mobile Device Forensics*, Revision 1.

xi) Monitoring and inventorying system locations, movement, connection status, and applications prior to and during an incident in order to aid the organization of malware response activities during a malware incident.

***[Eradication and Recovery Actions]***

**For All Information Systems:**

1) The SAISO, in coordination with SOs and IOs, for EPA-operated systems; and IOs, in coordination with SMs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Use automated eradication tools such as antivirus software, specialized malware removal utilities, patch management software and root-level inspection programs, as necessary to eliminate malware from infected systems and networks.

   b) Repair or rebuild infected hosts to guard against the spread or re-initiation of infections.

   c) Track and document all actions performed in order to contain or eliminate malware.

   d) Maintain Malware records at the designated official repository and at the site of the incident where on-site response teams report and take incident-related actions

   e) Maintain logs in accordance with *EPA Records Schedule 130*.

      i) Logs pertaining to a law enforcement action may subject them to retention requirements that are in accordance with *EPA Records Schedule 698*.

   f) Use EPA's Remedy system (or equivalent) as the Agency repository for tracking incidents reported through the EPA Call Center (EPA CC).

      i) The security incident component shall be separate from other tracking data to ensure only authorized personnel have access to the security incident information.

   g) Use workflow capabilities of EPA's Remedy system (or equivalent) to request incident response assistance from the ISOs and ISSOs.

   h) Provide access to the Agency's incident tracking database(s) for the OIG-OI to aid potential criminal investigative actions.

   i) Employ automated mechanisms to assist tracking of malware incidents, and collecting and analyzing information regarding security incidents.

      i) Report all known or suspected information security incidents or vulnerabilities immediately using the notification instructions located in IR-6, above. Once incident information is reported to CSIRC, the following actions shall be taken:

         (3) CSIRC shall conduct an initial inquiry to verify whether an incident actually occurred and provide immediate mitigation, if possible.

         (4) CSIRC shall record incident information in a tracking system.

         (5) Once an incident is validated, CSIRC shall determine the magnitude of the incident, determine who to notify, and in coordination with the SAISO, immediately escalate possible crime-related events to the OIG-OI.

ii) CSIRC shall coordinate informing other system personnel about an incident possibly affecting them in accordance with response actions and escalation protocols established for incidents.

(6) A CSIRC Coordinator collects and disseminates incident information by:

(a) Interfacing with the ISOs, ISSOs and US-CERT

(b) Reporting incidents to US-CERT, the OIG, Office of Public Affairs, the EPA Physical Security Officer, and EPA Senior Management, as appropriate.

## *APPENDIX C:* US-CERT and EPA INCIDENT CATEGORIES AND REPORTING TIMEFRAMES

| Category (CAT) | Name | Description | Reporting Timeframe |
|---|---|---|---|
| CAT 0 | Exercise / Network Defense Testing | This category is used during state, federal, national, and international exercises and approved activity testing of internal/external network defenses or responses. | **US-CERT**<br>Not applicable; this category is for each agency's internal use during exercises. |
| CAT 1 | *Unauthorized Access | In this category, an individual gains logical or physical access without permission to a federal agency network, system, application, data or other resource. | **US-CERT**<br>Within one (1) hour of discovery/detection.<br>**EPA CSIRC**<br>Incidents shall be reported to CSIRC immediately, no later than one (1) hour, after discovery and/or detection. These incidents can be reported via email or via telephone to any member of the CSIRC team. |
| CAT 1A | *Unauthorized Access | In this category, an individual gains logical or physical access without permission to a federal agency network, system, application, data or other resource containing PII data. | **US-CERT**<br>Within one (1) hour of discovery/detection.<br>**EPA CSIRC**<br>Confirmed or suspected incidents involving PII shall be reported immediately, no later than 59 minutes after discovery and/or detection. |
| CAT 2 | *Denial of Service (DoS) | An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DoS. | **US-CERT**<br>Within two (2) hours of discovery/detection if the successful attack is still ongoing and the Agency is unable to successfully mitigate activity.<br>**EPA CSIRC**<br>Incidents shall be reported to CSIRC within two hours of discovery and/or detection. |

| Category (CAT) | Name | Description | Reporting Timeframe |
|---|---|---|---|
| CAT 3 | *Malicious Code | *Successful* installation of malicious software that infects an operating system or application.<br>Note: Agencies are *__not__* required to report malicious logic that has been *successfully quarantined* by the anti-virus software. | **__US-CERT__**<br>Daily Note: Within one (1) hour of discovery/detection if widespread across the Agency.<br>**__EPA CSIRC__**<br>Incidents shall be reported within 24 hours of detection and/or discovery. If it is suspected that the outbreak of malicious code is widespread across the Agency, Category 3 incidents shall be reported within one hour of discovery. Incidents that fall into Category 3 shall be reported to CSIRC no later than the close of business of the last day of the current reporting month. Therefore, if a Category 3 incident occurs on the next to the last day of the month, it shall be reported to CSIRC by the end of the following day. |
| CAT 4 | *Improper Usage | A person violates acceptable use of any network or computer use policies. | **__US-CERT__**<br>Weekly<br>**__EPA CSIRC__**<br>Incidents shall be reported within one (1) week of detection and/or discovery. Incidents that fall into Category 4 shall be reported to CSIRC no later than the close of business of the last day of the current reporting month. Therefore, if a Category 4 incident occurs on the next to the last day of the month, it shall be reported to CSIRC by the end of the following day. |

| Category (CAT) | Name | Description | Reporting Timeframe |
|---|---|---|---|
| CAT 5 | Scans / Probes / Attempted Access | This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. | **US-CERT**<br>Monthly Note: If system is classified, report within one (1) hour of discovery.<br>**EPA CSIRC**<br>Incidents shall be reported to CSIRC by close of business on the seventh day of the following month. If the seventh falls on a weekend or holiday, the reporting requirement shall be close of business the next business day. If the system is a classified system, these incidents shall be reported within one (1) hour of detection and/or discovery. |
| CAT 6 | Investigation | Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. | **US-CERT**<br>Not applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated. |

*Any incident that involves compromised PII shall be reported to US-CERT within one (1) hour of detection regardless of the incident category reporting timeframe.