PREFACE TO SELECTED INFORMATION DIRECTIVES

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

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

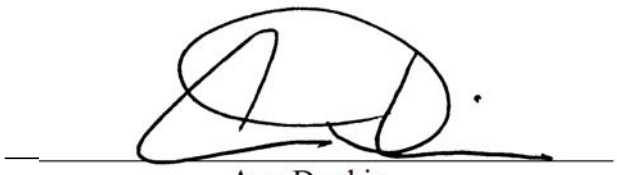
CHIEF INFORMATION OFFICER MEMORANDUM

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

Re-assigned CTO responsibilities

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

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



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

APPENDIX A

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

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

EPA INFORMATION PROCEDURES

OFFICE OF ENVIRONMENTAL INFORMATION

EPA Classification No.:	CIO-2150.3-P-08.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

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

INFORMATION SECURITY –
INTERIM INCIDENT RESPONSE PROCEDURES
V3.1
JULY 19, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Incident Response control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations.*

2. SCOPE AND APPLICABILITY

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

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

3. AUDIENCE

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that all offices within the Agency meet the minimum security requirements defined in the *Federal Information Processing Standards* (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems. All EPA information systems must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*. This chapter addresses the procedures and standards set forth by EPA, and in compliance with, the incident response family of controls found in NIST SP 800-53, Revision 3.

EPA Classification No.:	CIO-2150.3-P-08.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III*, Federal Information Security Management Act (FISMA)* as amended
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 USC 3501-3519)
- Privacy Act of 1974 (5 USC § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C— *Employees Responsible for the Management or Use of Federal Computer Systems*, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
- Office of Management and Budget (OMB) 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
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy

6. PROCEDURES

IR-2 – Incident Response Training

a. Appropriate role-based training must be provided on incident response responsibilities and procedures no less than annually.

   i. Incident response training must include user training in the identification

and reporting of suspicious activities, both from external and internal sources.

b. EPA CSIRC shall educate Information Security Officers (ISOs) and Information System Security Officers (ISSOs) and end users on CSIRC goals and operations.
    i. This training may be provided in various forms, including a CSIRC ISO/ISSO Handbook, security newsletters, intranet web pages, briefings, and instructor led training sessions.
    ii. All or a sub-set of end user incident response training must be included in EPA's annual awareness training.
c. Personnel with significant responsibilities for incident response shall take a minimum of eight (8) hours of incident response training annually.
    i. The eight (8) hours of training can count towards fulfilling role-based training requirements.
    ii. Incident response training must include tabletop exercises or offsite exercises as a part of actual Incident Response Plan testing.
d. The CSIRC Coordinator shall maintain a comprehensive electronic log of all Incident Response Plan related training.
    i. The electronic log must include names of participants, information system name(s), type of training, and date of completion.
e. Refer to *Information Security – Interim Awareness and Training Procedures* for requirements on role-based training.
f. NIST SP 800-50, 800-61, Revision 1, and 800-84 must be utilized as guidance on training personnel.

For high information systems

g. Simulated events must be incorporated into incident response training to facilitate the effective responses by personnel in crisis situations.
    i. Training environments must consist of automated mechanisms which simulate a live threat environment.
h. Automated mechanisms must be employed to provide a more thorough and realistic training environment.

IR-3 – Incident Response Testing and Exercises

For moderate and high information systems

a. The incident response capability must be tested and/or exercised annually and checklists reviewed quarterly to ensure all personnel are prepared to react to emergencies.
    i. Testing must include scenario-based exercises to determine the ability of the Agency to respond to information security incidents.
    ii. At a minimum, tabletop exercises must be performed; however, more robust functional exercises are recommended.
b. An Agency-level Incident Response Test Plan must be developed and reviewed and updated at least annually.
c. The results of incident response tests/exercises must be documented in the

Incident Response Plan.

i. The plan and test/exercise results must be reviewed at least annually.

d. The results of incident response tests/exercises must be used to identify and remediate weaknesses within the Incident Response Plan.

i. Corrective actions must be addressed in a Plan of Action and Milestones (POA&M).

e. NIST SP 800-84 and 800-115 must be utilized as guidance on test, training, and exercise programs for information technology plans and capabilities.

For high information systems

f. Automated mechanisms must be employed to more thoroughly and effectively test or exercise the incident response capability by:

i. Providing more complete coverage of incident response issues.

ii. Assisting in selecting more realistic test/exercise scenarios and environments.

iii. More effectively stressing the response capability.

IR-4 – Incident Handling

a. EPA's CSIRC shall define the processes by which the Agency prepares, detects, analyzes, contains, eradicates, and recovers from information security-related incidents such as computer viruses, unauthorized user activity, and serious software vulnerabilities.

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

b. CSIRC shall:

i. Protect EPA's information assets and network by responding to, mitigating, and resolving actual and potential incidents and events.

ii. Be available 24 hours a day, 7 days a week.

1. Personnel must be at a minimum immediately available during normal business hours and on call during the off-hours.

iii. Define response requirements for Agency reporting and response to information security incidents.

iv. Provide a service level for agency response to advisories that are received from external Computer Emergency Response Team (CERT) organizations and that may have a potential impact on Agency information systems.

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

vi. Respond to a reported incident according to defined response requirements.

vii. Provide management and logistical support to system administrators for timely reporting, tracking, resolving, and documenting detected information

security incidents.

viii. Coordinate with the Office of Technology Operations and Planning (OTOP) security staff as needed for logistical support.

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

x. Receive and forward all appropriate incident and vulnerability notifications (i.e. CERT) to the Information Owner (IO), System Owner (SO) and ISSO for respective system affected by the incident or vulnerability.

xi. Maintain a telephone contact list of system administrators, system managers, and ISOs to enable notification and coordination according to defined response requirements.

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

c. EPA's CSIRC shall maintain collaborative relationships with other internal EPA organizational units outside of the Network Security Operations Center (NSOC), including the following:
   i. Office of Inspector General (OIG) – Office of Investigations (OI)
   ii. Office of Public Affairs (OPA)
   iii. Human Resources
   iv. Facility (i.e., physical) security
   v. Congressional Affairs
   vi. Office of General Counsel (OGC)

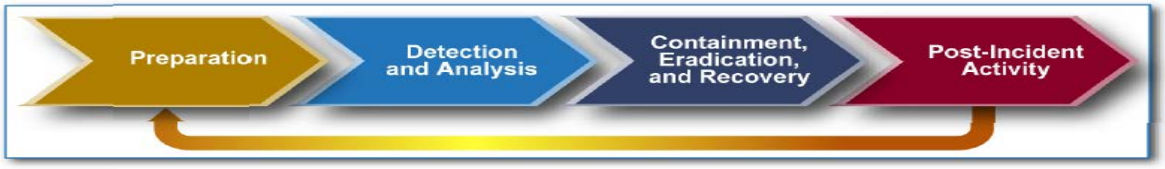
d. All personnel directly involved with incident handling (i.e., detection and analysis; notification; containment, eradication, and recovery; post-incident activities) shall sign a Non-Disclosure Agreement.
   i. Details of any incident must be discussed only on a need-to-know basis with authorized personnel.

e. ISOs, ISSOs and IT personnel shall assist in tracking, resolving, and documenting reported information security incidents, per CSIRC established SLA's and procedures.

f. NIST SP 800-36, 800-61, Revision 1, 800-83, 800-86, 800-92, 800-94, and 800-101 must be utilized as guidance on incident handling.

g. The security incident handling capability must be implemented to cover the full incident response life cycle:
   i. Preparation
   ii. Detection and analysis
   iii. Containment, eradication, and recovery
   iv. Post-incident activities

Figure 1 - Incident Response Life Cycle



Preparation

h. Information system personnel shall develop and maintain an Incident Response Plan that addresses all of the requirements within this chapter.
    i. The Incident Response Plan must also address the service levels established by EPA's CSIRC.
        - Refer to *Appendix B* for the categories and timeframes for various service levels.

i. EPA shall identify and establish incident response capabilities that enable EPA to respond when an event or incident occurs.
    i. EPA shall maintain lists of resources for incident response and handling.
    ii. Incident response resource lists must include the following:
        - Contact information, including cell-phone numbers and pager numbers for all appropriate personnel, including external sources such as other incident response teams representing other agencies and law enforcement.
        - Approved hardware and software tools for detection, analysis, eradication, containment, and recovery.
        - Relevant security resource reference materials (e.g., NIST SP 800-61, Revision 1; vendor-specific procedures for system recovery).

Detection and Analysis

j. Automated network management, vulnerability scanning tools must be used to help CSIRC in both proactive and reactive assessment and analysis of information security threats and vulnerabilities and detecting potential and actual security incidents.
    i. These tools must be used to assess compliance with information security policies, standards, and procedures.
    ii. CSIRC shall provide oversight and advisement services to the National Computer Center (NCC) for server security policy compliance assessment.
        - This service must involve use of vulnerability assessment tools such as ArcSight, EnCase, BigFix and other approved tools, as needed.
    iii. Automated network management tools must include intrusion detection systems (IDS) and firewalls.
        - IDS must be placed appropriately and used for near real-time alerting on potential incidents.
        - The log files of EPA's routers and firewalls must be regularly

reviewed to detect potential incidents as well as to assess the level of threat activity directed at EPA's network perimeter.

- All EPA servers, applications, routers, firewalls, and other networked devices must implement ArcSight logging functionality.

iv. Multiple layers of protection against email-borne viruses or other malware must be deployed, beginning at the firewall and mail routing hubs and ending at the workstation.

- CSIRC shall be responsible for managing and coordinating all incident responses to malware intrusions.

k. EPA shall employ methods and procedures to analyze potential and actual security incidents.

l. EPA shall implement operational procedures and a system to categorize incidents and escalate reports of incidents, alerts, and risks to the centrally managed IT infrastructure and the resources that rely on that infrastructure.

i. The Operational Status Categories during Alerts and Risks (OSCAR) system is used to categorize and escalate incidents.

ii. Procedures for escalating incidents shall be detailed according to Operational Status Categories.

- The six categories progress from low to high risk (OSCAR 0 through OSCAR 5).
- Refer to *Appendix C* for EPA's incident categories by type of incident.

iii. All suspected or confirmed incidents must be classified within categories 1 through 5 (category 0 is normal operations, with minimal risk).

- If a suspected or confirmed incident falls within multiple categories, the incident must be classified at the highest category that applies.
- The highest level (i.e., OSCAR 5) must only be invoked by the Chief Technology Officer (CTO) and must be coordinated with Continuity of Operations Plan (COOP) and disaster recovery efforts.

m. CSIRC shall escalate to the OIG-OI events comprising a criminal act.

n. CSIRC shall also report all information security incidents to United States Computer Emergency Readiness Team (US-CERT).

i. Reporting to US-CERT must be based on the incident categories and reporting timeframes detailed in *Appendix B*.

Detection and Analysis – Procedures for Sensitive Information

o. The following procedures must be adhered to when a Personally Identifiable Information (PII) security-related incident occurs or is suspected:

i. PII Incident Handling and Response Procedure, Chief Information Officer (CIO) 2151-P-06.

ii. Breach of Personally Identifiable Information (PII) Notification Response Procedures, CIO 2151-P-02.

Analysis and Legal Chain of Custody

p. All information and materials must be carefully collected, labeled, cataloged, and securely stored at each stage of intrusion analysis.

Containment

q. Countermeasures or strategies identified by EPA shall be used or put in place to mitigate threats or vulnerabilities, and shall balance the objectives of mitigation and data collection required for effective analysis and response activities. CSIRC shall maintain procedures for responses to specific types of incidents.

Forensics

r. Forensics shall be led by CSIRC and shall be performed in accordance with industry best practices designed to preserve evidentiary integrity of the data and shall encompass all data available which is related to the incident (e.g., firewall and other logs, system data, etc.).

s. ISO's shall perform forensic procedures locally under the direction of CSIRC when network-based forensic capabilities are not available or sufficient for forensic purposes.

t. The OIG-OI and the Office of Enforcement and Compliance Assurance (OECA) National Enforcement Investigations Center (NEIC) may be called upon to provide forensic assistance as needed.

Eradication and Recovery

u. After evidence preservation is completed, CSIRC shall take actions and provide guidance and assistance to ensure that elements of the incident are eliminated and the systems can be returned to normal operation.

Post-Incident Activity

v. The incident must be documented and reported within EPA:
   i. All incidents must have reports and forms finalized no later than 30 days after the close of the incident.
   ii. Incident response teams shall provide CSIRC with a copy of all related documentation.
   iii. A report that includes all activity, notifications, and actions taken during the incident must be forwarded to the appropriate management.

w. The Incident Response Plan(s) for the affected system(s) must be revised and updated.

x. Post-incident reviews must be conducted to learn from each incident experience and improve incident handling capabilities.

y. Lessons learned from incident handling activities must be incorporated into the incident response procedures and the resulting changes implemented accordingly.

z. Incident handling activities must be coordinated with contingency planning activities.

aa. Weaknesses and vulnerabilities must be addressed through the POA&Ms, when required.

For moderate and high information systems

bb. Automated mechanisms (e.g., online incident management system) must be

employed to support the incident handling process.

IR-5 – Incident Monitoring

a. Information system security incidents must be tracked and documented.

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

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

b. Electronic logs of all incidents that occur at EPA must 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.
    i. These logs must be maintained in accordance with *EPA Records Schedule 130*.
    ii. Logs pertaining to a law enforcement action may subject them to retention requirements that are in accordance with *EPA Records Schedule 698*.
c. EPA's Remedy system (or equivalent) must be used as the Agency repository for tracking incidents reported through the EPA Call Center (EPA CC).
    i. The security incident component must be separate from other tracking data to ensure only authorized personnel have access to the security incident information.
d. Workflow capabilities of EPA's Remedy system (or equivalent) shall be used by CSIRC to request incident response assistance of the ISOs and ISSOs to respond to those requests.
e. The OIG-OI shall have access to the Agency's incident tracking database(s) for actual and potential criminal investigative actions.
f. NIST SP 800-61, Revision 1 must be utilized as guidance on monitoring incidents.

For high information systems

g. Automated mechanisms must be used to assist in the tracking of security incidents.
    i. These automated mechanisms must 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, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs), or other electronic databases of incidents.

IR-6 – Incident Reporting

Note: The intent of this control is to address both specific incident reporting

requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations.

a. Security incident information must be reported to designated authorities.
    i. The type of security incident reported, the content and timeliness of the reports, and the list of designated reporting authorities must be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
    ii. Incidents must be reported within the timeframe indicated by the incident category.
        - See *Appendix B* for incident categories and mandatory reporting timeframes.
    iii. Incident reports must be submitted per the requirements in *Appendix B* even if the report is incomplete.
    iv. Violations involving national security information must be reported in accordance with Section 3 of EPA's National Security Information Handbook, Revision 1, December 2006.

b. All EPA personnel shall report all known or suspected information security incidents or vulnerabilities immediately.
    i. The preferred order of notification is:
        - Personnel shall notify the ISO immediately.
        - The ISO shall notify the EPA CC, who in turn will contact CSIRC.
    ii. If the ISO is not immediately available, then personnel shall immediately contact the EPA CC directly.

c. EPA CC must be the central point of contact for receiving reports of information security incidents.
    i. During normal duty hours, EPA CC employees shall:
        - Open a Problem Management Record (PMR) for each reported incident.
        - Route the PMR to the CSIRC Coordinator.
        - Forward all security-related calls to CSIRC.
    ii. Outside of normal duty hours, the EPA CC shall:
        - Maintain a Voice Response Unit (VRU) capability for after-hours reporting of information security incidents.
        - Automatically relay calls to the 24x7 network operations personnel who will contact the on-call CSIRC staff member.

d. Once incident information is reported to CSIRC, the following actions must occur:
    i. CSIRC team members shall conduct an initial inquiry to verify whether an incident actually occurred and provide immediate mitigation, if possible.
    ii. CSIRC shall record incident information in a tracking system.
    iii. Once an incident is validated, CSIRC shall determine the magnitude of the

incident and determine who to notify.

- CSIRC shall immediately escalate to the OIG-OI events that appear to be a criminal act.
- CSIRC shall coordinate informing other system personnel about an incident possibly affecting them, in accordance with response actions and escalation protocols established for incidents.

iv. A CSIRC Coordinator must collect and disseminate reporting about information security incidents. This activity requires:

- Interfacing with the ISOs and ISSOs.
- Interfacing with US-CERT.
- Other information security incident reporting and coordinating entities as necessary.

e. CSIRC shall report incidents to US-CERT, to the OIG, Office of Public Affairs, the EPA Physical Security Officer, and EPA Senior Management (e.g., Deputy Secretary, CIO), as appropriate for the incident and established reporting requirements in *Appendix B*.

Note: Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) 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.

f. Whenever there is a possibility of information system related criminal activity, the OIG-OI must be contacted.
   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 must be coordinated through the OIG.
   ii. All criminal-related information provided to outside agencies other than law enforcement must be reviewed by EPA's OGC.

g. Detected activities related to homeland security and/or counterintelligence activities shall be coordinated through the CSIRC with FBI, US Cert, and EPA's Office of Homeland Security.

h. Release of security-related incident information to any external entity, other than reporting to US-CERT, must be approved by the Senior Agency Information Security Officer (SAISO).
   i. Incident reports to external entities must be also approved by the Office of Technology Operations & Planning, Technical Information Security Staff (TISS) Director prior to the release.
   ii. All information provided to outside agencies must be reviewed by EPA's OGC.
   iii. All requests for information related to CSIRC activities must be forwarded to EPA's OPA, as approval by the SAISO.
      - Information is prohibited from being 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 must be considered confidentially sensitive and the property of the Agency.

i. Periodic summary incident reports must be submitted to individuals designated by the SAISO.

i. CSIRC shall provide other periodic information security reports to US-CERT as appropriate for the incident and established reporting requirements in *Appendix B*.

ii. ISOs and ISSOs shall forward the monthly collection of incident information to CSIRC, and CSIRC shall provide consolidated reports to the TISS Director.

iii. CSIRC shall ensure that any EPA reports including incidents related to EPA information within Line of Business Centers as determined by reporting procedures to avoid duplicate reporting.

iv. The scope of the monthly incident reports must include: detected scans, probes, and attempted accesses that are either internal to an EPA network or external to and directed at an EPA network.

v. The weekly incident report must include, to the extent possible, the following elements of the detected network activity:

- Incident date and time, including time zone.
- Indication of scan, probe or attempted access.
- Source IP, port, and protocol.
- Destination IP, port, and protocol.
- Operating System, including version, patches, etc.
- System function (e.g., Domain Name Server [DNS], web server, workstation).
- Antivirus software installed, including version, and latest updates.
- Physical location of the system(s) involved in the incident (e.g., Washington, DC).
- Method used to identify the incident (e.g., IDS, audit log analysis, system administrator).
- Impact to Agency.
- Resolution

j. NIST SP 800-61, Revision 1 must be utilized as guidance on incident reporting.

For moderate and high information systems

k. Automated mechanisms must be used to assist in reporting security incidents.

IR-7 – Incident Response Assistance

a. CSIRC shall serve as EPA's incident response support resource, integral to EPA's incident response capability, and offering assistance and advice to users regarding potential incidents and the incident handing and reporting procedures.
    i. These resources may include access to forensic services, if appropriate, or web-based support.

For moderate and high information systems

b. Automated mechanisms must be employed to increase availability of support features to users.
    i. Examples of mechanisms include automated answering and/or ticketing system for help desk, Really Simple Syndication (RSS) and Atom feeds, subscriptions, distribution lists, etc.

Note: 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 increasing understanding of current response capabilities and support.

IR-8 – Incident Response Plan

a. An Incident Response Plan must be developed 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 approach for 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 designated officials within the organization.
b. Copies of the Incident Response Plan must be distributed to personnel with significant incident response responsibilities incident response personnel elements.
c. The Incident Response Plan must be reviewed annually.
d. The Incident Response Plan must be revised to address system/organizational changes or problems encountered during plan implementation, execution, or testing.
e. Incident Response Plan changes must be communicated to incident response personnel and organizational elements personnel with significant incident response responsibilities.

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

7. RELATED DOCUMENTS

- NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, October 2003
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009
- NIST SP 800-61, Revision 1, *Computer Security Incident Handling Guide*, March 2008
- NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities,* September 2006
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006
- NIST SP 800-92, *Guide to Computer Security Log Management*, September 2006
- NIST SP 900-94, *Guide to Intrusion Detection and Prevention Systems (IDPS),* February 2007
- NIST SP 800-101, *Guidelines on Cell Phone Forensics,* May 2007
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008
- NIST SP 800-123, *Guide to General Server Security*, July 2008
- The National Strategy to Secure Cyberspace, February 2003 - www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

8. ROLES AND RESPONSIBILITIES

Director, Office of Technology Operations & Planning (OTOP)

a. The OTOP Director has the following responsibilities with respect to incident response:
   i. Ensure management and logistical support to IT personnel for timely reporting, tracking, resolving, and documenting detected computer security incidents.
   ii. Ensure coordination with the OTOP security staff as needed for technical support and direction required to provide management and logistical support to system administrators and to document the incident.
   iii. Ensure there are sufficient resources to implement and maintain an

effective centralized incident response capability.

Senior Agency Information Security Officer (SAISO)

a. The SAISO has the following responsibilities with respect to incident response:
    i. Ensure the CIO is informed of security incidents.
    ii. Ensure the organization has adequate procedures for information security incident handling.
    iii. Ensure the agency information security program adequately addresses incident handling responsibilities and procedures within the organization.
    iv. Coordinate with TISS Director to ensure incidents are adequately responded to.
    v. Coordinate evaluation and resolution of CSIRC mitigation recommendations.
    i. Coordinate with the Privacy Office and ensure privacy policies and procedures are followed when an incident involves PII.
    ii. Approve for release security-related incident information to any external entity, other than reports to US-CERT, FBI, or the intelligence community.

Computer Security Incident Response Capability (CSIRC)

a. CSIRC has the following responsibilities with respect to incident response and handling:
    i. Protect the Agency's information assets and network.
    ii. Work in conjunction with supporting entities to establish tools and resources in anticipation of security incidents and events.
    iii. Work with the community to make recommendations for securing networks, systems, and applications.
    iv. Educate ISOs and end users on CSIRC goals and operations.
    v. Define the process by which the Agency responds to computer security-related incidents such as computer viruses, unauthorized user activity, and serious software vulnerabilities.
    vi. Provide a service level for Agency response to computer security incident reporting.
    vii. Provide a service level for Agency response to advisories that are received from external CERT organizations and that may have a potential impact on Agency computer systems.
    viii. Provide a method to promote computer security awareness of related risks so the Agency is better prepared to handle those incidents and is protected against them.
    ix. Take actions to verify that an incident actually occurred upon learning of a potential incident.
    x. Determine the scope and impact of each intrusion and prioritize actions

accordingly.

xi. Determine the magnitude of the incident once an incident is validated.

xii. Maintain an electronic log of and track all incidents that occur at EPA.

xiii. 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.

xiv. Ensure that Remedy tickets for actual and potential incidents are:

- Updated throughout the incident management life cycle, and
- Made available only to appropriate personnel.

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

xvi. Periodically provide information security reports and updates to US-CERT.

xvii. Set up an incident support resource that offers assistance and advice to users regarding potential incidents and vulnerabilities and the incident handling/reporting procedures.

xviii. Manage and coordinate all incident responses to malicious software intrusions.

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

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

xxi. Assess impacts on EPA's security posture and controls as a result of handling and resolving incidents. Provide lessons learned for SOs, ISOs, ISSOs, senior managers and others with recommendations to mitigate weaknesses identified during analysis.

xxii. Determine specific response actions and escalation protocols for each incident.

CSIRC Operations Manager

a. The CSIRC Coordinator has the following responsibilities with respect to incident response:

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

ii. Facilitate annual incident response training for the CSIRC and IT security community supported by the EPA's Incident Response Plan.

iii. Maintain a comprehensive electronic log of all information security Incident Response Plan related training.

iv. Interface with the ISOs, US-CERT, OIG-IO and other law enforcement, as necessary.

v. 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.)

vi. Provide weekly incident reports to OTOP management and incident reports to US-CERT, as required.

Information Security Officer (ISO)

a. The ISO has the following responsibilities with respect to incident response:

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

ii. Respond immediately to a reported incident.

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

~~ii.~~ Follow-up with CSIRC and IT management to resolve and close outstanding incidents within SLA timeframes established by CSIRC.

iv. 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.

v. Develop, maintain, and publish procedures required for site-specific handling of computer security incidents as needed.

vi. Provide information on items such as the level of access an intruder gained and how the intruder was able to breach defenses.

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

viii. Maintain up to date contact information of SOs, site system administrators, system managers, and other security personnel. Provide the contact information to CSIRC and update as needed.

ix. Establish and maintain notification procedures for reporting computer security incidents at the site and to the OTOP security staff.

Information System Security Officer (ISSO)

a. The ISSO has the following responsibilities with respect to incident response:

i. Support the ISO in accomplishing ISO responsibilities for systems assigned.

Director of Technical Information Security Staff (TISS)

a. The Director of TISS has the following responsibilities with respect to incident response:

i. Provide oversight to CSIRC and incident management.

ii. Ensure a current telephone contact list of site system administrators,

system managers, and ISOs is maintained.

iii. Ensure that the EPA Incident Response Test Plan is reviewed and updated annually.

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

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

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

vi. Ensure computer security incidents are properly reported.

iii. Develops, distributes, reviews and revises an Incident Response Plan.

iv. Coordinates with SAISO to ensure incidents are adequately responded to.

v. Ensure senior managers, e.g., CTO, SAISO, are informed of incidents occurrences and their statuses in a timely manner.

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

EPA Call Center (CC)

a. The EPA CC has the following responsibilities with respect to incident response:

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

ii. Open a PMR for each reported incident.

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

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

National Computer Center (NCC)

a. NCC has the following responsibilities with respect to incident response:

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

ii. Direct any further immediate technical measures, as well as subsequent repair and resolution to the central and distributed email system components. Any subsequent communication necessary with the Lotus Notes administrators and ISO communities must be the responsibility of NCC.

iii. Expand the requirement for increased oversight and diligence in intrusion detection to include eight additional hours of near real-time sensor monitoring.

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

v. Identify, document, and maintain a database that includes all categorization, IO, SO and ISSO for respective system affected by the incident or vulnerability and applicable systems hosted by NCC.

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

a. OECA-NEIC has the following responsibilities with respect to incident response:
   i. Assist CSIRC and ISOs in forensic capabilities, when possible and needed.

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

a. OIG-OI has the following responsibilities with respect to incident response:
   i. Determine if an incident identified by CSIRC as possible criminal in nature is actually criminal in nature.
   ii. Serve as the primary point of contact for coordination with law enforcement.
   iii. Conduct criminal investigations of incidents when criminality is determined.
   iv. Assist CSIRC and ISOs in forensic capabilities, when possible and needed.

Office of General Counsel (OGC)

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

Office of Public Affairs (OPA)

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

Personal Computer Site Coordinator (PCSC)

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

System Administrator

a. System administrators have the following responsibilities with respect to incident response:
   i. Scan the information system(s) for actual data/document(s) and the presence of moderate and/or high sensitivity or PII information, if assigned to the incident.
   ii. 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, if assigned to the

incident.

iii. Evaluate the existence of interconnected information systems for additional possible unauthorized disclosure and/or distribution in partner networks, if assigned to the incident.

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

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

vi. Assume that storage devices accessed and backups conducted during the time of the incident are also contaminated.

vii. Isolate the server from the network if the network has been contaminated.

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

ix. Make a copy of the contaminated file if the network has been contaminated.

x. Collect all backup tapes, CD-ROMs, and/or disks of the contaminated systems if the network has been contaminated.

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 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 or 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.
- 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 EPA; external scanning refers to scans originating from a network that is not under the direct control and authority of 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 and includes a signature. The documentation can be accomplished manually or electronically.

10. WAIVERS

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

- substantive business case need(s)
- demonstration of, or a proposal for, establishment of adequate compensating

controls that provide a suitable alternative to the mandated protection

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

The SAISO and Director, OTOP shall coordinate to maintain central repository of all waivers.

11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

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

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

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

12. MATERIAL SUPERSEDED

EPA Information Security Manual, Directive 2195A1, 1999 Edition, Section 5

13. ADDITIONAL INFORMATION

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

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

APPENDIX A: ACRONYMS

CAT	Category
CC	Call Center
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
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
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
OGC	Office of General Counsel
OI	Office of Investigations
OIG	Office of Inspector General
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
SAISO	Senior Agency Information Security Officer
SIO	Senior Information Official

SO	System Owner
SP	Special Publication
TISS	Technical Information Security Staff
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team
VRU	Voice Response Unit
WAN	Wide Area Network

APPENDIX B: 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, international exercises and approved activity testing of internal/external network defenses or responses.	**US-CERT** Not applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	A person gains logical or physical access without permission to a federal agency network, system, application, data, or other technical resource.	**US-CERT** Within one (1) hour of discovery/detection. **EPA CSIRC** Incidents must 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	A person gains logical or physical access without permission to a federal Agency network, system, application, data, or other technical resource.	**US-CERT** Within one (1) hour of discovery/detection. **EPA CSIRC** Confirmed or suspected incidents involving PII must be reported immediately, no later than 59 minutes after discovery and/or detection.
CAT 2	*Denial of Service (DoS)	An attack that prevents or impairs the authorized use of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	**US-CERT** Within two (2) hours of discovery/detection if the successful attack is still ongoing and the Agency is unable to successfully mitigate activity. **EPA CSIRC** Incidents must be reported to CSIRC within two hours of discovery and/or detection.

Category (CAT)	Name	Description	Reporting Timeframe
CAT 3	*Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus software.	**US-CERT** Daily Note: Within one (1) hour of discovery/detection if widespread across Agency. **EPA CSIRC** Incidents must 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 must be reported within one hour of discovery. Incidents that fall into Category 3 must 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 must be reported to CSIRC by the end of the following day.
CAT 4	*Inappropriate Usage	A person violates acceptable use of any network or computer use policies.	**US-CERT** Weekly **EPA CSIRC** Incidents must be reported within one (1) week of detection and/or discovery. Incidents that fall into Category 4 must 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 must 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** Monthly Note: If system is classified, report within one (1) hour of discovery. **EPA CSIRC** Incidents must 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 must be close of business the next business day. If the system is a classified system, these incidents must 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** 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 must be reported to US-CERT within one (1) hour of detection regardless of the incident category reporting timeframe.

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.7	10/8/2008	Initial draft	Heather Flager	Procedures-IR-Draft_TO62_020_1
2.0	6/3/2009	Incorporated EPA comments	Heather Flager	Procedures-IR-Final_TO62_020_2
2.7	7/29/2010	Updated per NIST SP 800-53 Revision 3	Heather Flager	Procedures_IR_Draft.TO-062_050_1.0
2.8	7/20/2010	TISS comments and changes	Charleen Johnson	Procedures_IR_Draft.TO-062_050_1.0
2.9	1/12/2010	TISS Final Draft Review	Charleen Johnson	Procedures_IR_Draft.TO-062_050_1.0
3.0	5/2/2012	SAISO Final Review	Abe Getchell	Procedures_IR_Draft.TO-062_050_1.0
3.1	7/19/2012	Document Review	SAISO and LaToya Gordon	Procedures_IR_Draft.TO-062_050_1.0