Mandatory Reference: 545
File Name: 545mad_051503_cd32
Revision: 05/15/2003
Effective Date: 05/23/2003

Incident Response Guidance for Unclassified Information Systems

Recent Government Information Security Reform (GISR) legislation and regulatory guidance stress the importance of **incident response** in protecting information systems (IS). If an incident occurs, a prompt and coordinated response can limit damage, speed recovery, and help restore service to users.

A. Computer Security Incident

A computer security incident is an occurrence having actual or potentially harmful effects on an information technology (IT) system. The types of activity widely recognized as harmful include, but are not limited to, the following:

1. Attempts (either failed or successful) to gain unauthorized access to (or use of) a system or its data;

2. Unwanted disruption or denial of service;

3. Unauthorized changes to system hardware, firmware, or software, including adding malicious code (such as viruses); or

4. Detection of symptoms of the above, such as altered or damaged files, virus infection messages appearing during start-up, inability to log in, etc.

Note: Not every event that fits these definitions requires an incident response. For example, we expect routine attempts to send viruses into the system, and these are foiled daily by key countermeasures. Such expected and unsuccessful events do not need to be treated as computer security incidents.

On the other hand, incidents that are unexpected, are successful (or nearly successful), or indicate a new vulnerability, threat source, or motivation **must be reported**. Likewise, individual threats that cause an estimated harm of over $15,000 must be reported, even if expected or routine.

If there is doubt about whether to report an incident, it should be reported. The Computer Incident Response Team (CIRT) (see section B.6) will determine the level of response and documentation needed.

B. Incident Reporting Process

The following steps and the Incident Reporting Process Chart in Section C demonstrate the duties of system users, system administrators, and IS management when a suspected computer security incident occurs.

1. **Individual system user** duties include

    - Stopping all work on the computer;

    - At Missions, quickly reporting a suspected or actual incident to the local System Information System Security Officer (ISSO)[1] and System Manager;

    - In USAID/W, calling the IRM Help Desk at (202) 712-1234 or sending an e-mail from an unaffected computer to **irm-helpdesk@usaid.gov**; and

    - After business hours, calling the USAID Security Operations Center at (202) 712-5644.

2. **The IRM Help Desk** duties include

    a. In preparation for incidents

    - Maintaining an up-to-date list of USAID/W System Owners, System Managers/IT Specialists, and System ISSOs for each system. For the list of current ISSOs, see **Mission and System ISSOs** (this list is only available to those with USAID intranet access).

    - Developing procedures for handling after-hours calls regarding possible computer security incidents, including a phone message referring after-hours callers who need to report a possible computer security incident to the USAID Security Operations Center at (202) 712-5644.

    b. Identification

    - Creating a Remedy ticket regarding the possible incident; and

    - Notifying the appropriate System Managers or IT Specialists.

    c. After the CIRT resolves the incident or deems the anomaly a non-incident

    - Closing the Remedy ticket; and

[1] Mission ISSOs are considered to be System ISSOs

- Ensuring that the initial reporter of the incident and any others who may have been affected are aware that they may use their computer again.

3. **USAID Security Operations Center** duties include

   - Referring possible computer security incidents reported by Missions during non-duty hours to the first available IRM Security representative on the **Emergency Computer Security Incident POC List**[2]. (This list is Sensitive But Unclassified (SBU) and is only available to those with intranet access.)

4. **The System Manager/IT Specialist** of the system involved in the possible incident duties include

   a. Identification

   - Quickly and briefly investigating system anomalies to determine if a possible computer security incident is taking place or has occurred involving their system;

   - If the System Manager/IT Specialist determines the event is a possible incident, notifying the System ISSO and system owner; and

   - If the System Manager/IT Specialist believes the event to be a non-incident, notifying the IRM Help Desk.

5. **System ISSO** duties include

   a. Upon notification of a possible incident

   - Notifying and activating the Computer Incident Response Team (CIRT) based on the system involved (see Figure 1); and

   - Serving as the initial CIRT Team Chief. If more than one system is involved, the USAID ISSO becomes the CIRT Team Chief.

6. The **CIRT** consists of the System ISSO (the initial Team Chief for the incident), the System Manager, a computer security subject matter expert (SME) from the Emergency Computer Security Incident POC List, a core group of representatives called in for each platform involved, and the Bureau for Management, Office of Information Resources Management,

[2] System/Mission ISSO may call the Security Operations Center for Emergency Computer Security Incident POC names and phone numbers.

Telecommunications and Computer Operations Division (M/IRM/TCO) Network Operations Center (NOC) Manager if TCO systems are involved. (See Figure 1)

Figure 1 - Computer Incident Response Team

The duties of the CIRT include

a. Identification

- *Declaring the anomaly a non-incident and notifying the USAID ISSO at **isso@usaid.gov** and the IRM Help Desk at **irm-helpdesk@usaid.gov**; or
- Declaring the event a computer security incident.

b. Upon validation of an incident

- Instructing the user on whether and/or how to proceed;
- *Notifying the USAID ISSO at **isso@usaid.gov** within 24 clock hours;
- Identifying whether other systems are involved;
- Formulating a plan of action for containment and eradication, and recovery of systems and data;
- Assigning a priority level sufficient to ensure the availability of any required resources. Any resource designated must be exclusively dedicated to and focused on the investigation until the issue is concluded;
- Starting detailed documentation in an incident log, noting the event date and time, summarizing the anomaly, describing their own activities and those of a possible intruder or of malicious code, and documenting time and costs associated with resolving the incident; and
- *Promptly submitting initial and all subsequent reports, including information required for the Information Systems Security Incident Report (Section D of this reference), on the incident to the USAID ISSO at **isso@usaid.gov**.

c. During containment, eradication, and recovery

- Taking screen captures and/or snapshots of pertinent files within the first half-hour of any incident investigation (backing up files may also be required);

- Securing and protecting the affected system(s) and all related media as directed by the designated ISSO;

- Identifying risks to systems or data, including any significant operational impact caused by the computer security incident, and coordinating organization-specific issues that might affect any response plan their designated ISSO may need to communicate to the USAID ISSO;

- Continuing to investigate, report on, and mitigate the incident until resolution;

- Reducing/eliminating risk and cleaning up the system;

- Maintaining documentation; and

- *Notifying the IRM Help Desk at **irm-helpdesk@usaid.gov** and the USAID ISSO at **isso@usaid.gov** of the resolution.

d. Lessons learned

- Documenting notable lessons learned from the CIRT perspective and providing them to the USAID ISSO.

7. **The USAID ISSO** duties include

a. In preparation for incidents

- Identifying and assisting in the assignment of needed resources to support the CIRT;

- Communicating to all users of USAID information systems the incident response requirements outlined in this document; and

- Providing specialized training for personnel with specific Incident Response responsibilities.

b. During containment, eradication, and recovery

- Assisting the CIRT, and if more than one system is involved, assuming the position of CIRT Team Chief, and setting up an Agency-level CIRT;

- Notifying the Director, M/IRM, the Chief Information Officer (CIO), and the Director, Office of Security (SEC) of significant computer security incidents;

- Working with law enforcement, users, and/or System Administrators, network managers/administrators, and local designated ISSO(s) to advise on response actions;

- Collecting information from the CIRT required for the Information Systems Security Incident Report (Section D of this reference); and

- Submitting the Information Systems Security Incident Report, within a median time of five business days, on behalf of USAID to the General Service Administration's Federal Computer Incident Response Capability (FEDCIRC).

c. Lessons learned

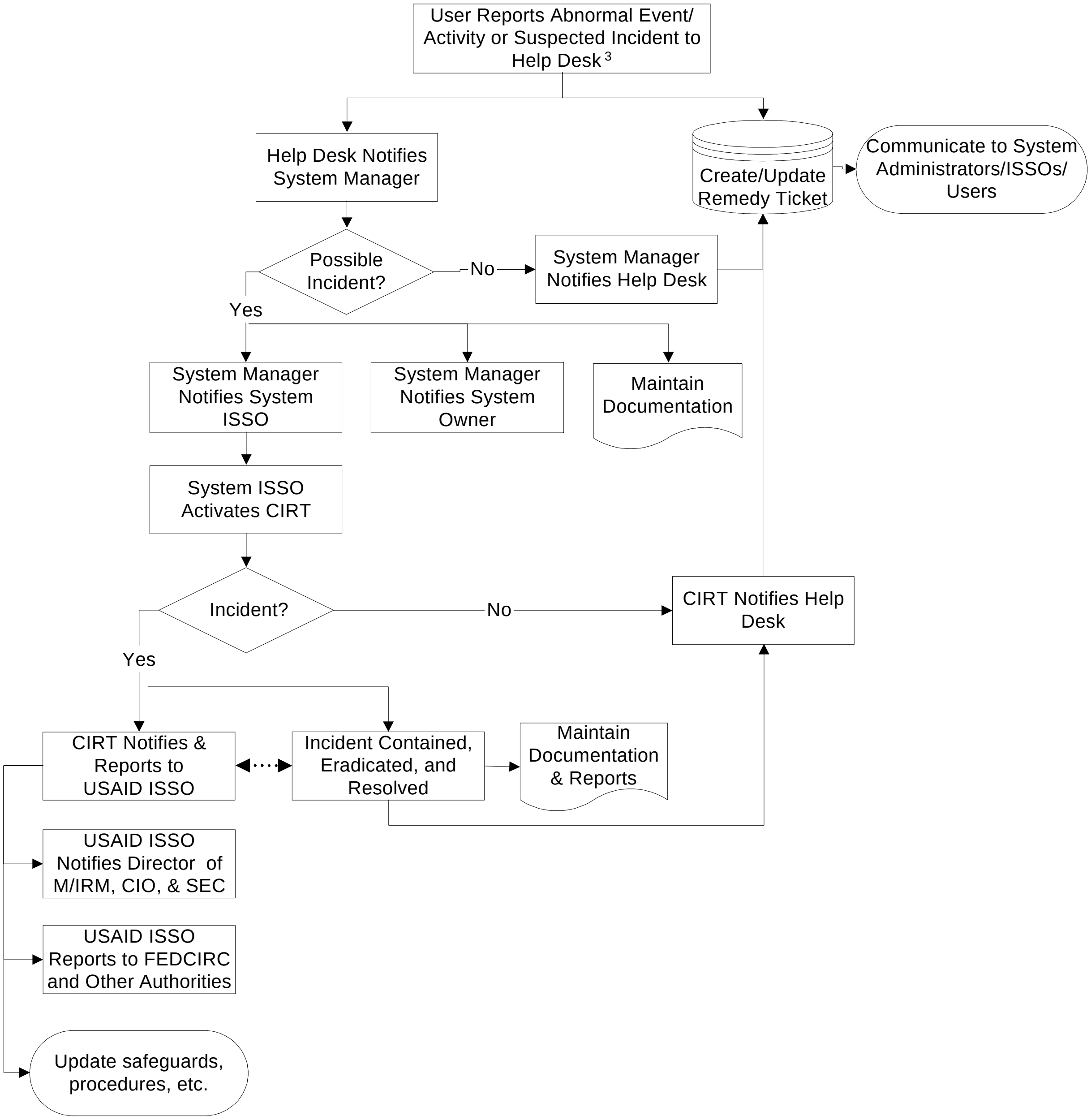
- Including lessons learned in security training and policy development; and

- Notifying the Office of Inspector General (OIG) about computer security incidents involving any apparent violation of laws, rules, or regulations.

The specific procedures contained in this Mandatory Reference have been coordinated with key offices, including the Office of the General Counsel (GC), SEC, OIG, and the USAID ISSO.

C. Incident Reporting Process Chart

The following Incident Reporting Process Chart outlines the duties of system users, system administrators, and IS management, as detailed in Section B.


User Reports Abnormal Event/ Activity or Suspected Incident to Help Desk [3]
Help Desk Notifies System Manager
Create/Update Remedy Ticket
Communicate to System Administrators/ISSOs/ Users
Possible Incident?
No
System Manager Notifies Help Desk
Yes
System Manager Notifies System ISSO
System Manager Notifies System Owner
Maintain Documentation
System ISSO Activates CIRT
Incident?
No
CIRT Notifies Help Desk
Yes
CIRT Notifies & Reports to USAID ISSO
Incident Contained, Eradicated, and Resolved
Maintain Documentation & Reports
USAID ISSO Notifies Director of M/IRM, CIO, & SEC
USAID ISSO Reports to FEDCIRC and Other Authorities
Update safeguards, procedures, etc.

[3] Please note that procedures may be different in Missions or when calling after hours at USAID/W. Please see paragraph B.1 for details.

D. United States Agency for International Development Information Systems Security Incident Report

Incident Number: ____________ Category (defined below): 1 2 3 4 5 6 7 8

Date of Incident: ________________________ Time of Incident: ______________________________

1. Reporting Organization Information:

Organization: ____

Name: ____

Section: ____

Telephone #: ____

E-mail Address:____

2. Target Host Information:

Host IP:____

Host Machine Name: ____

Classification Levels:

Classified ____________ /Sensitive But Unclassified ____________ /Non-Sensitive _____________

System Mission: ____

Operating System: ____

3. Source(s) Information:

Source(s) IP: ____

Source Host Name: ____

Source Name and Address: ____

4. Intrusion Information:

Type of Incident or Attack: ____

How Detected: ____

Description of Incident: ____

Was System Compromised? Yes ________ No _________

Impact on Operation: ____

Countermeasure(s):____

5. Notification:

Network Administrator: ____

Firewall Administrator:____

LAN Administrator: ____

Network Security: ____

Virus Section:____

Information Systems Security Officer: ____

Federal Computer Incident Response Team:____

Law Enforcement Agency:____

Incident Category Definitions:

Cat #	Definition	Cat #	Definition
1	Unauthorized Root / Administrative Access	5	Poor Security Practice
2	Unauthorized User Access	6	Unauthorized Probe / Information Gathering
3	Unauthorized Attempted Access	7	Malicious Logic
4	Denial of Service	8	Misuse