Incident Identification and Reporting Procedures

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545map_060106_cd44

Information System Security
Incident Identification and Reporting Procedures
for Users, Help Desk Staff, and Information System Security Officers

1. Introduction

This document defines the processes that you must follow during security incident identification, reporting, and escalation.

2. Incident Identification

An incident is a risk made real—the result of a threat that exploits or attempts to exploit a vulnerability.

USAID personnel are responsible for identifying and then reporting possible security incidents. You are the Agency's first line of defense. Some security incidents may seem to be normal problems; others require review and analysis to confirm. You may not be able to determine if specific activity is a security incident, but any abnormal event should be reported. Some common, unexplained events that you should report are:

- Password changes you didn't initiate (you can't log in) or requests to share your password,
- E-mail activity to you or that is received in your mailbox,
  - Responses to e-mail that was not sent by you,
  - Large volumes of spam, or
  - Large numbers of messages you didn't send
- Browser home page changes or pop-up ads that can't be closed,
- New desktop icons appearing at login,
- Inability to connect to USAID or Internet servers (web- or application-sites),
- Workstation infection from a virus, worm or Trojan, adware, or spyware
- Sudden workstation slowdowns,
- File additions, changes, or deletions,
- Noticeable decreases in hard drive space, or
- Sudden increases in hard drive or network activity.

You must report these and other suspicious events immediately to your local Help Desk, system administrator, or ISSO.

3. Pre-Reporting Guidelines

Five general guidelines that you should follow during a possible security incident are:

- If your password has been compromised, change it immediately and then report the incident as documented in the User Incident Reporting section of this document.
- Do not continue working. Where possible, gracefully stop working in any applications that you are using and save your work to a network drive.
- Do not close any applications or shutdown the system.
- Do not resume using the application or system until it is declared "safe" by the incident response team.
- Do not discuss the security incident, except with the incident response team.

4. User Incident Reporting

During a possible security incident, time, activities, and attention to detail are important. You must record and communicate details as quickly and as accurately as possible. They are the facts upon which USAID will respond, and they will be important if USAID needs to escalate the incident. Necessary details include:

- Your identifying information (name, location, telephone number and workstation),
- A description of the suspicious activity,
- How the suspect activity differs from normal activity,
- The date(s) and time(s) on which the activity occurred, and
- Any other information which can be gathered without affecting or worsening the situation or notifying a potential or confirmed intruder that you are aware of his or her presence.

You should report incidents to your local system administrator or Help Desk, your local ISSO, or the USAID ISSO. You should report the incident by telephone. You may use the form, **Computer Security Incident – User Report** (CSI-UR).

[Note: This document is only available on the USAID intranet. Please contact **ads@usaid.gov** if you need a copy.]

An incident, such as a denial of service, may interrupt or prevent e-mail or forms submission—the important action is to notify your support staff as quickly as possible. You may contact the USAID Help Desk at (202) 712-1234 or the USAID ISSO by e-mail to **ISSO@usaid.gov**.

The flowchart in Section 7 is a depiction of the incident reporting process for the local Help Desk, System Administrators, and ISSO.

5. System Administrator and Help Desk Handling and Reporting

The system administrator or Help Desk must gather the information related to the event. The user must provide this information, or the system administrator can obtain it from the form or e-mail. The system administrator or Help Desk must conduct a preliminary review to determine if the event is a security incident. If it is a security event, a review must be conducted to determine the incident's severity level. The USAID ISSO must be informed of the incident specifics. The USAID ISSO will review them, and may alter the assigned security level of the incident.

If the incident is determined to be of Level Three severity (as determined from the Incident Severity Table or assigned by the USAID ISSO) it should be handled without escalation to the USAID ISSO. The system administrator must conduct an analysis and take remedial action. You must complete a **Computer Security Incident – Analysis Report** (CSI-AR) and a **Computer Security Incident – Resolution Report** (CSI-RR).

[Note: These documents are only available on the USAID intranet. Please contact **ads@usaid.gov** if you need a copy.]

When the incident has been resolved, you must forward a copy of the CSI-UR, CSI-AR and CSI-RR to the USAID ISSO.

If the incident is determined to be of Level Two severity and if it can be handled locally, the procedures for a Level Three severity incident can be followed. If the incident cannot be handled locally, a Remedy ticket must be created and assigned to ISSO Security group (this can be done by the Help Desk or the USAID ISSO), and the CSI-UR and CSI-AR (if started) must be sent to the USAID ISSO. For all Level Two severity incidents, ISSO closure is required.

If the incident is determined to be of Level One severity, it must be forwarded to the USAID ISSO immediately, with a Remedy ticket (created as for a Level Two incident), and the CSI-UR and CSI-AR (if started) must be sent to the USAID ISSO. For all Level One severity incidents, USAID ISSO closure is required.

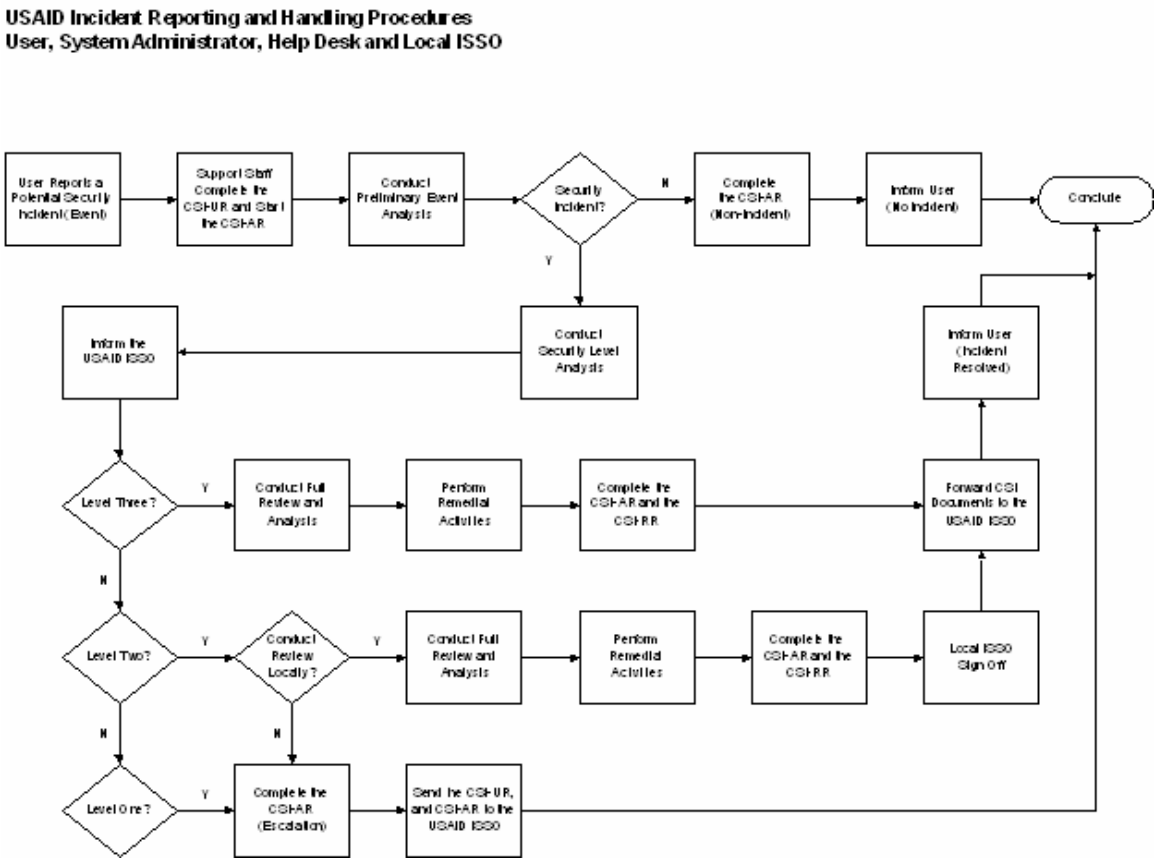
6. Incident Severity and Handling

The following table summarizes the four incident severity categories, and the actions that USAID needs to take at each severity level.

Severity	Description	Handling Procedure
Level Zero	User reported event.	CSI-UR completed and initial review and analysis conducted to determine if the event is a security incident, and if so, the severity level assigned to the incident.
Level Three	Incident effects are localized, no more than one or two users or computers, and not affecting any major USAID system. Examples include non-mailing viruses, receipt of Spam, and spyware or adware.	Local personnel handle all incident response from analysis through to completion. CSI-AR and CSI-RR are completed. All CSI forms are sent to the USAID ISSO after incident resolution.
Level Two	Incident effects may be localized, but the event affects several (more than two) users or disrupts normal work for the system or affects the local area network (LAN). Examples (local) include a virus outbreak that affects LAN drives or a local denial of service, and (non-local) an e-mailing virus, or ***any event that the USAID ISSO declares to be a Level Two incident.***	If the response can be handled locally, the handling procedures for Level Three apply. If the response cannot be handled locally, all documentation is sent to the USAID ISSO for analysis and resolution. ***For all Level Two severity incidents, ISSO signoff at resolution is required.***
Level One	Incident effects are not localized, large number of users, a Mission, the USAID enterprise, or external networks are affected. Examples include spamming e-mail viruses, successful hacking attempt, major system shutdowns, etc. or ***any event that the USAID ISSO declares to be a Level One incident.***	Incident analysis and response will commence locally; however, the USAID/W ISSO staff will be notified and respond. If necessary, the incident will be escalated to federal reporting and law enforcement entities. ***For all Level One severity incidents, USAID ISSO signoff is required before recovery.***

7. Incident Reporting Flowchart

We also describe the incident reporting process for the local Help Desk, System Administrators, and ISSO in the following flowchart.



The above graphic uses standard flow chart symbols to illustrate the steps and decisions involved in incident reporting and handling as described in the text of this document.