ADMINISTRATIVE COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION

DEPARTMENTAL HANDBOOK

Distribution:
All Department of Education Employees

Approved by: _____/s/_____
Michell Clark
Assistant Secretary for Management

Handbook for Information Security
Incident Response and Reporting Procedures

For technical questions concerning information found in this ACS document, please contact Eric Eskelsen at Eric.Eskelsen@ed.gov or on (202) 245-6530.

Supersedes OCIO-14, Information Security Incident Handling Procedures dated 5/13/2005.

FOR OFFICIAL USE ONLY

U.S. Department of Education

Office of the Chief Information Officer

Handbook for Information Security Incident Response and Reporting Procedures

Information Assurance Program

TABLE OF CONTENTS

1 Introduction

1.1 Purpose

This document provides incident response and reporting procedures to ensure appropriate and expeditious handling of information security incidents[1] that may affect the U.S. Department of Education's (Department) normal business operations. These procedures define the Department's incident response and reporting process as well as roles and responsibilities. The intended audience of this document is all Department personnel, but it focuses primarily on system users. This document provides a high level overview of the Department's capability and carefully explains the importance of communication and staff involvement in all phases of the process. Personnel should reference this guide for procedures to assess incidents, coordinate and communicate with relevant Department personnel, and fulfill reporting requirements to achieve effective and timely responses to security incidents.

1.2 Background

An incident response and reporting capability serves as a mechanism to receive and disseminate incident information, and also provides a consistent capability to respond to incidents as they occur. As defined by National Institute of Standards and Technology (NIST) Special Publication 800-61: Computer Security Incident Handling Guide, a computer security incident is "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."[2]

1.3 Scope

The incident response procedures apply to all Department employees and contractors.

1.4 Document Structure

This document contains four major sections and five supplemental appendices. Sections two (2) and three (3) address the cyber incident response and reporting procedures, and should be employed as the primary action-oriented sections of this document. Section four (4) discusses the roles and responsibilities of those participating in the incident response and reporting process. The appendices include a computer security suspicious event form and a chain of custody form to be used during incident handling. The appendices also include the following reference materials that may be helpful to incident handlers and users: a list of common acronyms, definitions of common incident response terms, and a list of suspicious events.

[1] See appendix E for definition of an Incident

[2] See appendix H for a list of references

2 Incident Response Procedures

2.1 Definition

The Department is adopting the NIST Special Publication 800-61 definition of a computer security incident: "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." Typically, the incident response life cycle consists of six stages:

(1) *Preparation:* Establish an approach to incident response, to include defining incidents, developing policy and procedures, and identifying and implementing other components required for responses.

(2) *Detection/Identification:* Analyze detection components (e.g., intrusion detection systems, firewalls, audit logs) to identify signs of an incident and verify that an incident has occurred, notify appropriate officials, and safeguard evidence to ensure a verifiable chain of custody.

(3) *Containment:* Stop the incident before it spreads or causes more damage.

(4) *Eradication:* Identify and mitigate the cause of the incident (e.g., un-patched system) and components of the incident (e.g., malicious code).

(5) *Recovery:* Restore affected systems to an unaffected state and validate them in terms of functionality and security.

(6) *Follow-up:* Develop follow-up reports; extract lessons learned for the Incident Management Program, and update policies, procedures, and other elements as necessary.

Response activities involve the entire Department--everyone has a role and associated responsibilities within the incident response life cycle. It is essential that one individual be the primary point of contact for the incident response activities undertaken to contain, eradiate, and recover from an incident. The Office of the Chief Information Officer (OCIO) Information Assurance Services (IAS) Office manages the Department of Education's Computer Incident Response Capability (EDCIRC). The EDCIRC Coordinator serves as the primary focal point, Department-wide, for incident reporting and escalation activities.

In an incident response and handling effort, several other individuals and groups may need to be involved. During an incident there will typically be one person that ensures that response and handling procedures are followed (referred hereafter as an Incident Handler) while there is another (potentially the same person) that is responsible for the reporting and escalation activities to the EDCIRC Coordinator or his designee (referred hereafter as an Incident Coordinator). At the discretion of the EDCIRC Coordinator or designee, the Office of Inspector General (OIG)/Technology Crimes Division (TCD)/Computer Crimes Unit (CCU) may also be involved. The OIG/CCU may provide additional investigative and forensic capabilities. The CCU is part of the OIG's Information Technology Audits and Computer Crimes Investigation (ITACCI) team. For the purpose of this document the Computer Crimes Unit will be referred to as CCU. Other primary groups involved in incident response are system users and support personnel. The rest of this section describes the actions to be taken by each group during an incident.

2.2 Office of Inspector General

It is the mission of the OIG to promote the efficient and effective use of Department resources in support of American education. To this end, the OIG provides independent and objective assistance to the Congress and the Secretary in ensuring continuous improvement in program delivery, effectiveness, and integrity.[3] OMB FISMA guidance also requires the OIG to evaluate Department FISMA data, including security reviews and Plan of Action and Milestones (POA&M) statements. These evaluation results are then incorporated into the annual FISMA report. This review is part of the OIG mission to act as an independent auditor and conduct periodic reviews of the Department's systems for legal and regulatory requirements.

The OIG component responsible for investigating computer security incidents is the Computer Crimes Unit (CCU), which falls under the Assistant Inspector General for Information Technology Audits, and Computer Crime Investigations (ITACCI). The CCU performs cyber criminal investigations in response to attacks against, as well as unauthorized access of, Department information systems networks, databases, and computer communications systems. The CCU also investigates the criminal misuse of Department computers, which could include the accessing of child pornography. In addition to conducting criminal investigations, the CCU performs forensic analysis of computer media in support of criminal investigations. The CCU consists of Special Agents with a formal technical background working alongside other technical professionals assigned to the unit. All computer crime investigators have full statutory law enforcement authority as granted by Congress.

Incidents that must be reported to OIG:

Incidents that may constitute a computer crime (violations of applicable Federal and/or State laws) must be reported to the OIG. Examples of the types of incidents that must be reported include, but are not limited, to the following:

- Compromise of systems privileges (root access);
- Compromise of information protected by law;
- Unauthorized access of Department IT systems and/or electronic data;
- Exceeding authorized access of Department IT systems and/or electronic data;
- Denial of service of major IT resources;
- Child pornography; and
- Malicious destruction or modification of Department data and/or information (website defacement).

[3] Refer to the Department of Education Web Page: http://www.ed.gov/about/offices/list/om/fs_po/oig/intro.html for additional information

CCU cannot investigate a computer security incident without receiving a timely incident report. The failure to provide OIG timely incident reports may directly impede the criminal investigative activities of the CCU staff. If incidents are not reported as soon as possible, the Department may lose information that is vital to the securing of evidence, as well as, making important connections to ongoing cases and making decisions about initiating new cases.

2.3 System User Response Activities

The Department has many complex systems used on a regular basis by employees and contractors. The daily activities of nearly every job require interaction with some of these systems. Because system users (users) are the people most familiar with the normal operation of the systems, users play an important part in detecting and reporting unusual behavior that may be a sign that an incident has occurred. Also, when systems are directly affected by an incident, users could play an active role in the response process by assisting security and incident response staff members. The following items explain what users should expect to happen during each of the phases of response efforts and what users' responsibilities are during each phase.

2.3.1 Preparation

Users are typically not involved in most preparatory measures, such as developing incident response procedures. However, users are required to attend training and awareness activities that cover incident reporting processes and procedures.

2.3.2 Detection/Identification

Users play a key role in detecting incidents because they are often the first to see signs of suspicious activity. Users should report all suspicious activity immediately to the appropriate System Security Officer (SSO). The table below provides examples of suspicious signs that users might encounter and provides a possible explanation for each sign. (Appendix F contains a more complete list of suspicious signs.) The example text is indicative of how users could initially describe these events to a SSO. When reporting an incident, the user should provide as much information as possible, including point of contact information, the approximate time the event was observed, computer identification information (e.g., asset tag number), and a brief description of the event.

Once the user notifies the SSO of the observed activity, it will be reviewed and evaluated to determine if an incident has occurred, and if so, the level of the threat and the potential scope of the incident. The Incident Handler and Incident Coordinator are responsible for determining if an incident has occurred and what actions should occur to contain, eradicate, and recover from the incident. (Further details of the Incident Handler and Incident Coordinator roles are available in Section 4 of this document.) Users are also responsible for documenting any and all actions they perform related to an incident, including those actions directed by support personnel.

Table 2.0, Examples Of Suspicious Event Indications That System Users May Encounter

Example	Possible Event Description	Possible Incident Type
Files are missing on a workstation.	Unexplained modification or deletion of data	Unauthorized Access
A known working password no longer works.	Inability of one or more users to log in to an account	Unauthorized Access
A user receives an email message not originating from the Help Desk that requests actions to be taken to protect systems from a virus.	A virus/worm email hoax	Malicious Code
A user is unable to log in to an account.	Successful or failed attempt to compromise a user account	Unauthorized Access
Unauthorized personnel are using restricted resources.	Misuse of system resources by valid users	Unauthorized Access
An unusual error message is displayed on the screen.	Unexplained attempts to write to system files or changes in system files	Unauthorized Access, Malicious Code
Irregular activity occurs, such as sporadic opening of programs.	Unusual usage patterns	Unauthorized Access, Malicious Code
An unknown individual solicits an employee for personal or proprietary information.	Attempts to "Social Engineer" or otherwise convince users/administrators to provide information to unauthorized parties	Other

2.3.3 Containment

Users often participate in containment efforts because they typically have immediate local access to the workstation or other devices that may have been attacked. This allows users to act quickly which limits the damage caused by the attack, and to preserve valuable evidence related to the attack. The actions taken by the user may significantly impact the state of the evidence. For this reason, all efforts should be made to preserve any evidence of the suspicious activity.

Support personnel (i.e. Help Desk, CSO, SSO. etc…) can direct users to take any of the steps described below to assist in containing and preserving evidence. If there is any question as to what action should or should not be taken, the user should contact the Computer Security Officer (CSO) and the SSO for additional guidance. Any actions taken by the user must be reported to the CSO and the SSO as soon as they are taken.

Users whose workstations are involved in an incident should complete the following steps:

- **Do not shutdown the workstation by using the power button or the operating system's shutdown features!** In some instances shutting down your workstation or using the operation system's shutdown feature operation may cause further damage.

- Contact the Help Desk at 202-708-HELP (4357) for assistance. Help Desk staff can assist personnel in determining the type of incident that has occurred and how to best handle it.

- If information is currently being taken or destroyed or the system is actively being used to attack other systems, disconnect the workstation from the network by physically removing the network connection from the workstation (physically disconnecting the network cable from the workstation) as soon as possible. Help Desk staff can assist you in this matter, if this action is necessary.

- Contact the office CSO and the SSO for the affected system. The CSO listing can be found by going to ConnectED, References and Resources, Directories and Contacts, ED Directories.

- Do not attempt to copy files off the computer or to identify further evidence of the incident unless specifically directed to do so. Taking such action on a running computer can destroy evidence which can be key to determining what occurred and identifying the responsible party.

- Contact the Incident Coordinator to validate the occurrence of an incident.

If the Incident Handler or Incident Coordinator determines that the incident might result in a future investigation by OIG-CCU, the Incident Handler or Incident Coordinator need to immediately contact their CSO to contact the EDCIRC Coordinator or his designated backup prior to unplugging the system. The EDCIRC Coordinator or his designated backup will consult with OIG-CCU. CCU needs to be involved from the beginning to ensure that all potential evidence is preserved. The OIG-CCU Duty agent is available to the EDCIRC Coordinator and his designated replacement 24x7 for consultation on these matters. The EDCIRC Coordinator and his designated backup have received the Duty Agent Roster from the IG.
If the affected system is a laptop, the user should seek forensic guidance immediately from the Help Desk. Improper power disconnection (e.g., unplugging the laptop and removing the battery for an extended period) can drain the backup batteries and cause loss of data, which can cause admissibility issues should the laptop be considered evidence in a criminal investigation. Therefore, it is important to seek forensics guidance before any action is taken.

The best approach for handling the laptop is to call the Help Desk for guidance on performing the following steps:

- Disconnect the power cord.
- Remove the battery.
- Remove the hard disk drive.
- Replace the battery.
- Plug the power cord back in and maintain the battery's charge, as soon as possible.

If users suspect that their Personal Digital Assistants (PDA's) are involved in an incident, they should shut off the PDA as soon as possible, and report the incident to the SSO, CSO, and Help Desk.

2.3.4 Eradication

Users typically do not perform any activities during the eradication stage. However, users should be aware that their systems might need to be modified as part of eradication, such as running antivirus software, applying patches to applications, or even reinstalling the operating system.

Any actions taken by the user must be reported to the appropriate SSO in order to prevent any loss of evidence and coordinate response efforts. It is important to note that systems may be unavailable to users during some eradication activities.

2.3.5 Recovery

The goal of the recovery stage is to restore all functions and data to a known good state. Users may participate in recovery only when directed to do so by the CSO, the SSO, or Incident Handler. The user may be asked to test systems and applications to ensure that they are working properly and that the data is current and complete, as well as performing other actions to validate that recovery was successful. Test and other results must be reported to appropriate support personnel, as the results are available. These results are then incorporated into reports and provide feedback on the success of recovery efforts.

2.3.6 Lessons Learned

Users rarely participate directly in the Lessons Learned process, although in some cases, a user who was pivotal in a particular incident may be asked to participate to a limited extent. Users indirectly see the results of this phase through improvements to the incident response process and to policies, procedures, technologies, and other components of the Department improvements that were identified through earlier Lessons Learned efforts.

2.4 System Support Personnel Response Activities

System support team leads and managers define the actions required of each group and individual system support personnel, who are responsible for their respective area of expertise. Specific responsibilities and activities are detailed in the incident procedures of each support group. The Incident Handler and Incident Coordinator manage the response efforts of all these teams. In addition to the activities described below, system support personnel will also maintain a chain of custody that demonstrates who did what when, including clearly documenting each transfer of evidence (e.g., date, time, persons involved). This is especially important in preserving any physical evidence that may be analyzed by the OIG/CCU or law enforcement. Furthermore, no changes should be made to any physical evidence. Preservation of evidence is an important element of the incident response process. The following items explain what system support personnel can expect to do during each of the incident response phases.

2.4.1 Preparation

The System Security Officer and the Computer Security Officer develop and maintain a foundation to support a system-level incident handling capability. The preparation activities consist of, but are not limited to, developing policy and procedures, identifying supporting roles and responsibilities, and establishing and implementing supporting tools and processes to ensure timely reporting of and response to security incidents. The procedures should include specific directions to ensure that appropriate documentation and chain of custody for evidence are maintained.

Additionally, regular communication through routine activity reports is an essential component of the preparation stage. To this end, support personnel are required to collect, maintain, and report system metrics. This baseline information is important in providing a means to distinguish unusual

patterns of activity and in identifying and addressing system anomalies. The information collected may include a baseline of "controlled" observation to more easily identify unauthorized network traffic. System metrics should be consistent with Department reporting requirements as well as verified with the EDCIRC Coordinator to ensure consistent meaningful measurements across department systems. See section 3.0 Reporting Procedures for information on reporting requirements to the EDCIRC Coordinator.

2.4.2 Identification

In incident identification, the SS) should first coordinate with network services to determine whether the suspicious event may have been caused by a mis-configuration, outage, or other benign action. Incident Handlers should begin by gathering and reviewing network, system, and application logs. Often these logs can provide insight into an incident without ever touching the affected system.

Once it has been confirmed that a security incident has occurred, the Incident Handler should oversee the incident response effort and ensure that the system's incident response procedures are followed while the Incident Coordinator is responsible for communicating incident-related information and escalating the incident, as appropriate, to Management and EDCIRC Coordinator. The EDCIRC Coordinator reports to the appropriate internal and external parties, such as the OIG/CCU. During the identification stage, the Incident Handler and Incident Coordinator are responsible for classifying the incident based on two key factors (described below) along with other supporting information:

Threat Determination: The Incident Handler and Incident Coordinator work with appropriate support groups to research the reported event and determine the threat that the activity represents to the relevant systems and to the Department as a whole. If the threat is serious, the participation of additional personnel may be needed to determine the scope of the threat.

Scope Determination: Once the threat is classified as requiring a response, the scope is determined relative to its overall impact to the Department's mission and functions. Other factors are part of the process of determining the scope, such as how many systems and users the reported event may affect.

Figure 3.1 (pg. 13) provides a schedule for reporting incident information to the EDCIRC Coordinator.

2.4.3 Containment

Once the incident is reported appropriately in accordance with Figure 3.0, containment activities to stop the incident from spreading or causing more damage may commence. To prevent any damage to evidence, containment activities should be coordinated with the OIG/CCU. All actions taken during the response process must be recorded and reported. In determining the risk of continuing to operate the affected systems, users are responsible for assisting as directed. However, system support personnel will perform most containment activities, such as the following:

- Documenting all actions performed during the response.

- Keeping all Incident Handlers informed and advising the appropriate parties (e.g., system owners) of progress.

- Ensuring that active measures are taken to stop an ongoing incident (e.g., firewall rule set modifications, email filtering, system disconnection).

- Performing two disk images of a system onto unused media, verifying the integrity of the images, and safely storing the second image for future use as evidence.

- Gathering and reviewing network, system, and application logs.

- Changing passwords on compromised systems and systems that interact with the compromised systems.

2.4.4 Eradication

Eradication is the process of identifying the cause of the incident and mitigating that cause, as well as removing components of an incident. It is important to note that eradication may destroy evidence of the incident and the OIG/CCU must be involved. Any steps taken in the eradication process must be documented.

Examples of eradication actions include running an antivirus program to remove infected files, applying patches to a system, and modifying a firewall rule set to block the usage of a particular network service. The eradication process is chiefly the responsibility of system support personnel, however, users may assist as needed. If the cause of the incident cannot be determined, a best guess based on the evidence at hand should be made and included with the initial report.

2.4.5 Recovery

Once the system appears to be performing normally, it must be tested and validated before placing it onto a production network. Every effort must be made not to keep or restore backdoors or malicious code during recovery. For example, if a root kit installation is suspected, the system should be reformatted and the operating system should be rebuilt, including all patches and fixes, prior to redeployment. Users may need to verify that the system is functioning properly before it resumes operations. Applications and data may also need to be reloaded on the fresh operating system. Recovery steps are to be recorded and reported up the chain to include the EDCIRC Coordinator and the OCIO/CCU.

2.4.6 Follow-Up

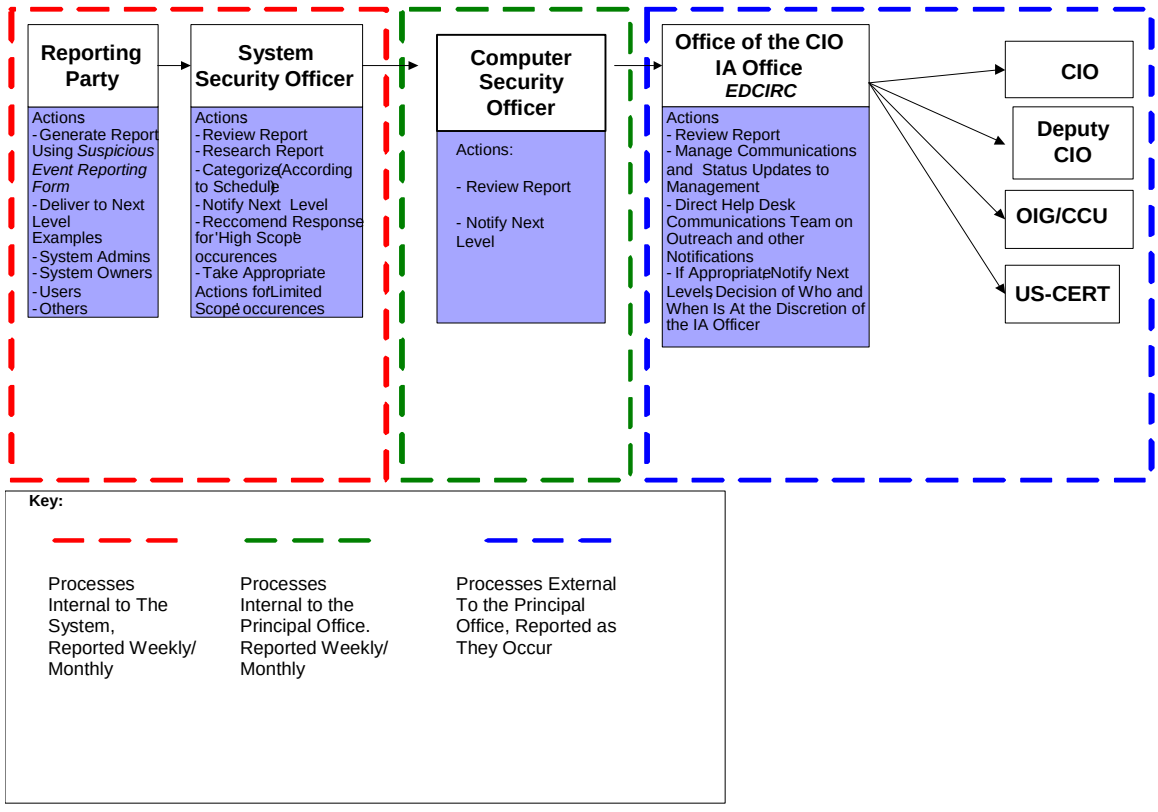
A follow-up report is written to collect and consolidate previous reports and documents. This must be completed as soon as possible after the incident to ensure a full and accurate account of all details. The most significant incidents require lessons learned meetings to discuss the incident and actions taken in response to it. These lessons feed back into the Incident Management Program, which leads to improvements in both the incident response process and in the Department's policies, procedures, technologies, and other components. Refer to Figure 3.1 for specific report delivery requirements.

3 Reporting Procedures

Each employee and contractor of the Department is responsible for reporting suspicious events that could be an incident. Any observed event that may indicate a computer security incident must be reported immediately to the relevant SSO or security administrator by telephone, email or fax.

Additional reference material is available at the Information Assurance Intranet Web site. This site provides a resource for Department personnel wishing to locate security information, policies, and applicable forms for reporting suspicious events and/or incidents pertaining to the Department. The Information Assurance Intranet Web page is located at the Information Assurance Intranet site. The Information Assurance email box may also be used to report incidents to IT Security personnel. The Information Assurance email box address is EDComputerSecurity@ed.gov.

Figure 3.0, Department Incident Reporting



3.1 EDCIRC Incident and Event Reporting Process

EDCIRC, as a function of the Department's IA office, contains a number of components, including the Department's communication, coordination, reporting, analysis and management capabilities that relate to computer incidents and threats. The EDCIRC Coordinator is responsible for directing these tasks across the Department and is central to the efficiency and success of each of the components. Incidents must be reported to the EDCIRC Coordinator per occurrence, and events must be reported on a weekly and monthly basis. **Specific requirements for the reporting of incidents and events are explained in this section.**

Incident Management is a complex process that integrates many security players into a cohesive program. EDCIRC manages this program capability for the Department to respond to computer security incidents. The involvement of each group is dependent on various factors such as the nature of the threat or incident, as well as where the group falls within the incident response lifecycle. Due to its adaptable structure, EDCIRC is not described as comprising specific entities, but is embodied primarily in the duties of the EDCIRC Coordinator combined with the appropriate support teams as needed. For example, an incident or threat involving a virus would not necessarily require the involvement of the messaging team unless email is an attack vector. The specific role of the EDCIRC Coordinator and associated reporting requirements are described in sections 3.0 and 4.5.4.

EDCIRC operates in accordance with the Distributed Incident Response Team Model definition[4] described in NIST Special Publication 800-61. This model recognizes that the Department is a complex organization with responsibilities distributed among staff and contractor support teams. However, each is required to report to and coordinate EDCIRC per sections 3 and 4 of this document.

The following section provides guidelines on reporting to the EDCIRC Coordinator, including a list of possible incident and event categories.

3.1.1 Incident Reporting

The CSO and Network Security Officer are required to report incidents to the EDCIRC Coordinator per occurrence. Incidents that involve Personally Identifiable Information (PII) data must be reported to the Federal incident response center (US-CERT) **within one hour of discovery**. This includes loss of information in electronic or physical form, whether or not it is a suspected or confirmed breach. To facilitate timely reporting incidents involving PII should be reported immediately to the EDCIRC Coordinator. All other incidents should be reported as outlined in Figure 3.1. All reportable incidents containing sensitive, but unclassified information, need to be encrypted prior to submission. This may be accomplished via point-to-point encryption. Figure 3.1 provides a list of the incident categories and the reporting timeframes for

4 *Distributed Incident Response Team Model:* The organization has multiple incident response teams, each responsible for handling incidents for a particular logical or physical segment of the organization. This model is effective for large organizations (e.g., one team per division) and for organizations with major computing resources at distant locations (e.g., one team per geographic region, one team per major facility). However, the teams should be part of a single centralized entity so that the incident response process is consistent across the organization and information is shared among teams. This is particularly important because multiple teams may see components of the same incident or may handle similar incidents. Strong communication among teams and consistent practices should make incident handling more effective and efficient.

each incident. The following listing (derived from US-CERT's *Federal Incident Reporting Guidelines*) provides examples of the incident categories to be used in classifying the incident type:

Malicious Code: Successful virus, Worm, Trojan horse, or other code-based infection on a device (report number of devices infected per occurrence). If an infection is prevented, it would be reported as an event.

Scans/Probes/Attempted Access: Requests sent to another system to gain information that **pose a serious threat** to a critical system by relaying information to be used in a subsequent attack. If probes or scans do not pose a serious threat to a critical system, they would be reported as events.

Denial of Service: A successful attack that is intended to prevent or impair the authorized use of networks, systems, or applications by exhausting resources.

Unauthorized Access: A person gaining logical or physical access without permission to a network, system, application, data or other resources; examples include root compromise, unauthorized alteration of data, and Web site defacement.

Inappropriate Usage: A person violating acceptable computing use policies.

High impact incidents are a greater priority and thus require more rigorous reporting and response actions. However, the overall impact of an incident is directly related to the criticality of the system affected by the incident. US-CERT provides guidelines for determining the severity of impact and assigns appropriate priority levels to reflect the extent of an incident's impact in relation to criticality[5]:

[5] Impact definitions adopted from *FedCIRC Incident Reporting Guidelines*, http://www.us-cert.gov/federal/reportingRequirements.html, September 21, 2004 and merged with system criticality definitions outlined from the Department of Education, *Handbook for Information Technology Security, Certification and Accreditation Process*, February 2003.

Figure 3.1, Federal Agency Incident Categories[6]

Category	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.	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	Within one (1) hour of discovery/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.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	*Improper Usage	A person violates acceptable computing use policies.	Weekly
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.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

Appendix B, the Computer Security Suspicious Event Form, provides a complete list of information that should be gathered if possible. However, as some information is not available until the incident is closed out, minimum requirements are provided below for each stage. Initial suspicious event reports should contain the following minimum information:

- Name
- Contact information
- System affected (IP address, host name, OS, etc)
- Incident type (i.e. malicious code, probes and reconnaissance scans, denial of service, unauthorized access)

[6] Impact definitions adopted from Federal Incident Reporting Guidelines, http://www.us-cert.gov/federal/reportingRequirements.html, July 25, 2006.

- Incident Handler and contact information (if different than above)
- Estimated time of resolution (where possible)
- Event assessment
- Actions taken

Additional information and updates should provide:

- Response Activity Summary
- Impact change (if applicable)
- Additional systems affected (if any)
- Updated time to resolution (if possible)

The final report should include specific information on the response activities taken and the results of those actions. Information on the hardware and software specifications should also be included. Refer to Appendix B for the full Computer Security Suspicious Event Form.

Additionally, if incidents involve PII (Personally Identifiable Information) the Computer Security Suspicious Event Form for PII data needs to be submitted as well. Refer to Appendix C for the full form.

3.1.2 Major System or Network Vulnerability Reporting

In addition to reporting on incidents, the CSOs and Network Security Officer are required to report major system or network vulnerabilities to the EDCIRC Coordinator per occurrence within 30 minutes of detection or notification. These vulnerabilities require immediate attention to determine remediation as continued exploitation could have a large impact to the Department and result in major system or network outage. Examples include router, firewall, or network operating system vulnerability.

3.1.3 Network Analysis Reports

Network traffic analysis reports are to be submitted on a regular basis to the EDCIRC Coordinator. The two reports described below provide baseline information for determining anomalous behavior within Department networks.

Report daily the top 10 IP addresses that generated more than 40 MB of inbound or outbound traffic during the previous day. This can be generated automatically using network-monitoring tools such as Webtrends.

Report weekly (on each Monday or the week's first workday) internal and perimeter firewall log information from the previous week showing the lowest eight hours of traffic volume per day.

3.1.4 Weekly Summary Reports

The CSOs and Network Security Officer must generate weekly reports for the EDCIRC Coordinator. Weekly reports summarize the past week's event activity, and may include changes to point of contact (POC) information, improvement suggestions, and other incident response issues of immediate concern. Weekly reports are due each Monday (or the week's first workday) for events that occurred during the previous weeks.

Events in the weekly summary report should be categorized as follows:

- Malicious Code Prevented. An infection from a virus, worm, Trojan horse, or other type of malicious code was prevented and did not cause any harm to any system.
- Inappropriate Usage. The Department's acceptable computing use policy was violated, or other misuse of resources occurred.
- Other. Cannot be reported in an above category.

3.1.5 Biweekly Summary Reports

Biweekly reports summarize the detected scans for the past two weeks events, and may include changes to POC information, improvement suggestions, and other incident response issues of concern. The biweekly summary report collects probes and reconnaissance scans that were determined not to be causing a threat to a critical system. Biweekly reports are due to the EDCIRC Coordinator every other Monday (or the week's first workday) for events that occurred during the previous two weeks.

3.2 OCIO Reporting Requirements

Incident reporting internally and externally is an OCIO function. The EDCIRC Coordinator is responsible for ensuring that incidents are reported up to the CIO, as well as to external entities such as the OIG/CCU and US-CERT. The OCIO serves as the interface to external organizations as well as a Department-wide coordination point.

3.2.1 Reporting to Internal Entities

The EDCIRC Coordinator is responsible for aggregating reports into a Department-level sanitized monthly summary report, which is then sent to relevant Department management. OCIO will also collect additional information to support its Department-wide correlation of threats, vulnerabilities and incidents.

3.2.2 Reporting to External Entities

Upon notification of incidents, the EDCIRC Coordinator will report these incidents to US-CERT. Information requests to Department management from US-CERT must be submitted through EDCIRC to ensure consistent reporting across the Department. The EDCIRC coordinator will provide a copy of the incident handling monthly report to the OIG/CCU. The Department monthly incident report will assist the OIG/CCU in reporting to other law enforcement agencies as needed (i.e.a summary presentation report of Department Computer Security incidents to the President's Council on Integrity and Efficiency (PCIE), the FBI, etc.)

4 Incident Response and Reporting Roles and Responsibilities

This section outlines the incident response roles and responsibilities of all personnel involved with Department IT systems. While all Department employees and contractors are responsible for reporting incidents and following incident response procedures, several Departmental positions entail specific responsibilities.

4.1 Employees and Other System Users

Employees' and other system users' responsibilities include:

- Reporting security problems, suspicious events, and incidents to their respective SSO or other appropriate security officer;
- Reporting viruses, password security, and rules-of-behavior violations to their respective SSO or other appropriate security officer; and
- Following other response procedures as outlined in section 2 of this document.

4.2 System Administrators and Network Security Officers

The responsibilities of System Administrators and Network Security Officers include:

- Ensuring that the SSO/CSO is aware of all matters that concern the security of the systems for which they are responsible;
- Participating in the handling of an incident as needed;
- Conducting regular log reviews and audits; and
- Identifying and reporting to the SSO/CSO any inconsistencies or irregularities in log entries or other signs that may signify a security incident.

4.3 EDNET

The EDNet Information System Security Incident Response Plan provides guidance to the EDNet technical staff in effectively addressing IT security incidents and promptly addresses the user's needs when a security incident occurs. The CIO will designate, if necessary, an Incident Handler and Incident Coordinator for EDNet when an incident occurs, otherwise, the EDNet Network Security Officer and/or OCIO CSO may fill these roles. This section documents incident reporting responsibilities within EDNET.

4.3.1 Incident Handler

The individual assigned to the Incident Handler role will vary based on the nature of the incident. The system Incident Handler is responsible for:

- Recording all information as the team suspects that an incident has occurred;
- Following established procedures for evidence gathering and handling;
- Ensuring system-level incident response procedures are followed; and
- Providing the Incident Coordinator with timely updates for communication to Department management.

4.3.2 Incident Coordinator

The individual assigned to the Incident Coordinator role will vary based on the nature of the incident. The Incident Coordinator is responsible for:

- Communicating incident-related information;
- Raising the incident, as appropriate, to Management and the EDCIRC Coordinator;
- Providing updates throughout the incident response effort; and
- Ensuring the Suspicious Event Form(s) are completed, updated, and submitted to the EDCIRC Coordinator.

4.3.3 System Security Officer

The System Security Officer's incident reporting responsibilities include:

- Responding to reports of possible incidents;
- Reporting incidents to the appropriate CSO; and
- Performing corrective actions as directed in response to a reported incident.

4.3.4 Computer Security Officer

The Computer Security Officer's responsibilities include:

- Ensuring the reporting of internal incidents to the EDCIRC Coordinator;
- Providing the weekly and monthly event reports to the EDCIRC Coordinator; and
- On an as-needed basis, assisting with and/or facilitating their resolution.

4.3.5 EDNET Network Security Officer

The EDNET Network Security Officer is responsible for:

- Ensuring that the System Security Officer/CSO is aware of all matters that concern the security of EDNET;
- Reporting incidents to the EDCIRC Coordinator;
- Providing the weekly and monthly event reports to the EDCIRC Coordinator; and
- Performing corrective actions as directed in response to a reported incident.

4.4 Systems External to EDNET

All systems external to EDNET must establish and maintain incident handling guidelines specific to that system. Owners/operators of contract owned networks are responsible to inform the Incident Coordinator, the CSO and the SSO for that system, as to who will be Incident Handler for that system. This section documents incident reporting responsibilities.

4.4.1 Incident Handler

The individual assigned to the Incident Handler role will vary based on the nature of the incident. The system Incident Handler is responsible for:

- Ensuring system-level incident response procedures are followed; and
- Providing the Incident Coordinator with timely updates for communication to Department management.

4.4.2 Incident Coordinator

The individual assigned to the Incident Coordinator role will vary based on the nature of the incident. The Incident Coordinator is responsible for:

- Communicating incident-related information;
- Raising the incident, as appropriate, to Management and the CSO;
- Providing updates throughout the incident response effort; and
- Ensuring the Suspicious Event Form(s) are completed, updated, and submitted to the EDCIRC Coordinator.

4.4.3 System Security Officer

The System Security Officer's incident reporting responsibilities include:

- Responding to reports of possible incidents;

- Reporting incidents to the appropriate CSO; and
- Performing corrective actions as directed in response to a reported incident.

4.4.4 Computer Security Officer

The Computer Security Officer's responsibilities include:

- Ensuring the reporting of internal and external (as appropriate) incidents to the EDCIRC Coordinator;
- Providing the weekly and monthly event reports to the EDCIRC Coordinator; and
- On an as-needed basis, assisting with and/or facilitating their resolution.

4.5 Office of the Chief Information Officer

The OCIO has primary responsibility for ensuring the Department has a Computer Incident Response Capability.

4.5.1 CIO

The CIO is responsible for:

- Reporting and advising senior Department management on computer incidents and if any incidents are harmful and may prevent any Departmental activities from being performed (i.e. ed.gov website is/will be down for a day for repair);
- Ensuring that a comprehensive Departmental incident-reporting and escalation program has been developed and implemented;
- Establishing policies and procedures governing the reporting and resolution of internal incidents; and
- Approving information regarding incidents for release to outside organizations.

4.5.2 Deputy CIO

The Deputy CIO works closely with the CIO and, at times, serves as his/her designee. The Deputy CIO is responsible for:

- Ensuring the implementation of the Department's incident reporting program;
- Ensuring the implementation of the Department's policies and procedures governing the reporting and resolution of internal incidents; and
- Acting as the CIO's designee for approving information regarding incidents for release to outside organizations.

4.5.3 Director, Information Assurance Services

The Director, Information Assurance Services (IAS) maintains the following responsibilities:

- Conducting periodic risk assessments of systems and applications;
- Ensuring each system maintains its own incident handling capability;
- Ensuring incidents are reported and escalated appropriately to internal and external entities;
- Training all Departmental employees in the skills necessary to recover from, preserve evidence of, and/or prevent security breaches to systems in order to help the OCIO fulfill the mission of security;

- Capturing and reporting department-wide incidents;
- Generating incident metrics;
- Providing analysis of systemic or root causes with recommendations;
- Raising incidents to the CIO; and
- Designating the EDCIRC Coordinator and EDCIRC Coordinator Backup positions.

4.5.4 EDCIRC Coordinator

The EDCIRC Coordinator is responsible for:

- Reporting incidents internally and externally;
- Compiling and sanitizing the appropriate reports;
- Reporting all privacy related incidents to the Department's Privacy Advocate and collaborating with affected officials on incident response activities;
- Coordinating incident response and reporting activities across the Department; and
- Other duties referenced in Appendix G.

4.5.5 EDCIRC Coordinator Backup

The EDCIRC Coordinator Backup is responsible for:

- Covering for the EDCIRC Coordinator when the EDCIRC Coordinator is not available; and
- Assisting the EDCIRC Coordinator in the EDCIRC Coordinator duties as needed.

4.5.6 Director, Security Services

The Director, Security Services is responsible for:

- Establishing and administering two security functions on a Department-wide basis:

  (1) Personnel Security and Suitability; and
  (2) Information Security - as it relates to classified national security information;

- Coordinating with the Chief Information Officer in assuring the security of ED's computer hardware and information systems;
- Initiating background investigations for applicants, appointees, employees, and contractors; and

- Conducting periodic internal reviews and evaluations as part of an ongoing departmental self-inspection program related to the handling and safeguarding of classified national security information.

4.5.7 OCIO Communications Team

The OCIO Communications Team is responsible for coordinating the development and approval of the communications to Department customers in the event of a network or system outage.

4.6 Office of Inspector General/Technology Crimes Division (TCD)/Computer Crimes Unit (CCU)

The OIG/CCU is responsible for:

- Conducting audits, inspections, and criminal investigations when warranted. (CCU Special Agents maintain arrest powers);

- Investigating computer crimes, conducting forensic analysis, maintaining chain of custody, and preserving evidence resulting from computer crimes and abuse or misuse of system resources; and

- Determining those organizations (internal and external) with which to share information. OIG/CCU is the Department's primary law enforcement liaison with other law enforcements entities to the Department.

4.7 Office of Management

4.7.1 Senior Agency Official for Privacy

The Assistant Secretary for Management is the Department's Senior Agency Official for Privacy, and has overall responsibility and accountability for ensuring the Department's implementation of information privacy protections, including the agency's full compliance with Federal laws, regulations, and policies relating to information privacy, such as the Privacy Act.

4.7.2 Privacy Advocate

The Privacy Advocate provides senior level support to the Assistant Secretary for Management who serves as the Department's Senior Agency Official for Privacy. The Privacy Advocate coordinates and facilitates the development and evaluation of policy proposals relating to the Department's collection, use, sharing, disclosure, and protection of personally identifiable information.

Appendix A. Acronyms

CIO	Chief Information Officer
CSIRT	Computer Security Incident Response Team
DoS	Denial of Service
DDoS	Distributed Denial of Service
EDCIRC	Department of Education Computer Incident Response Capability
EDNet	Department of Education Network
FISMA	Federal Information Security Management Act
IDS	Intrusion Detection System
IT	Information Technology
MAC	Media Access Control
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG/CCU	Office of Inspector General/Computer Crimes Unit
OMB	Office of Management and Budget
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
POC	Point of Contact
US-CERT	United States Computer Emergency Readiness Team

Appendix B. Computer Security Suspicious Event Form

Please note that if you are having difficulty printing this form a copy of it may be obtained at the Information Assurance website.

US Department of Education Computer Security Suspicious Event Report ***(Final or Preliminary Report: _____)***					
This form is for use by Department of Education personnel to escalate potential computer or network security events to the Office of the Chief Information Officer					
Contact Information					
Name		**Title**		**Organization**	
Address					
Phone		**Fax**		**E-mail**	
Location Information					
Building Number		**Room Number**		**Rack/Cube Location**	
Time Information of Incident					
Date		**Time**		**Time Zone**	
Loss or suspected loss of Personally Identifiable Information (PII)? Yes___ No___ *If yes, please complete the Computer Security Suspicious Event Form for PII in Appendix C.*					
Classification of the Suspicious Activity					
	Denial of Service		Web Site Defacement		Social Engineering
	Virus / Malicious Code		User Account Compromise		Hoax
	System Misuse		Other Intrusion		Network Scanning/Probing
	Technical Vulnerability		Root Compromise		Other /Specify:
	Theft/Loss of Equipment		Physical Security Violation		Other/Specify:
If a Virus, Provide the name(s) of the virus(es): Provide any URL with information specific to this virus: Provide a synopsis of the incident: Actions taken to disinfect and prevent further infection:					
If a Technical or Physical Vulnerability, Describe the nature and effect of the vulnerability in general terms: Describe the conditions under which the vulnerability occurred: Describe the specific impact of the weakness or design deficiency: Indicate whether or not the applicable vendor has been notified: **If equipment has been lost or stolen,** Provide details on the type of data or information stored on the equipment, impact of loss and state whether the incident has been reported to authorities (include report number if provided.) and any other details.					
Host and/or Network Information related to the Suspicious Activity					
IP Address		**Host Name**		**OS**	**Apps**
Additional Host/Network Information: (Versions, Releases, Security Logging,)					
IP Address of Suspected Source:					
Source IP		**Source IP Resolution**		**Reason Suspected as Source**	
Incident Assessment: Is this incident a threat to life, limb, or a critical agency service? Yes No If yes, please elaborate: Sensitivity of the data residing on system: Damage or observations resulting from incident: Yes No					

Actions Taken: (1) What actions have been taken on the system (Back-ups, commands, removed from network, etc). (2) Who has been notified? Times? Other info:
Additional Information: (If this incident is related to a previously reported incident, include any previously assigned incident number for reference.):
System logs are attached below (firewall logs, IDS logs, and any other applicable supporting artifacts)

Appendix C. Computer Security Suspicious Event Form for PII data

Please note that if you are having difficulty printing this form a copy of it may be obtained at the Information Assurance website.

US Department of Education Computer Security Suspicious Event Report *For Actual or Suspected Personally Identifiable Information Incidents* ***(Final or Preliminary Report: _____) Date: / /***					
Contact Information for Incident Handler					
Name		**Title**		**Organization**	
Address					
Phone		**Fax**		**E-mail**	
Building Number		**Room Number**		**Rack/Cube Location**	
Time that loss of data was realized					
Date		**Time**		**Time Zone**	
Narrative of Incident					
Description of data that was lost					
Was data on Mobile Media? Yes, No If yes what type?					
	Laptop		DVD		Magnetic Tape
	CD		Thumb Drive		Other/Specify:
Was Data Encrypted? _____Yes _____No **Were local authorities contacted? _____Yes _____No** **Is there a police report? _____Yes _____No (If so please attach it below)** **Number of Individuals impacted? _____**					
Has notification of Individuals started? If so, explain how/what has started.					
Actions Taken to reduce the problem from happening again: (1) What actions have been taken on the system (Back-ups, commands, removed from network, etc). (2) Who has been notified? Times? Other info:					
Additional Information: (If this incident is related to a previously reported incident, include any previously assigned incident number for reference.):					

System logs/Police Report are attached below (firewall logs, IDS logs, and any other applicable supporting artifacts)

Appendix D. Chain of Custody Form

DEPARTMENT OF EDUCATION **INFORMATION SECURITY AND PRIVACY** **PROPERTY AND CHAIN OF CUSTODY DOCUMENT**			Case Number	
Name and Title From Whom Received			Address and Telephone Number	
Location Where Obtained			Reason Obtained	Date/Time Obtained
Item #	Quantity	Description of Articles		
		Chain of Custody		
Issue	Date	Released By	Received By	Reason
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
Location _____			Property Number _____	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	

		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	

FINAL PROPERTY/EVIDENCE RELEASE AUTHORITY (release authorization must be signed by the OCIO, OIG or Legal)

Items(s) _____ on this document pertaining to the investigation involving _____ _____ is/are no longer required as evidence and may be disposed of as indicated below.

(Printed Name/Title) (Signature) (Date)

Released to Owner or Other (Name/Address) _____

Destroyed by (describe) _____

Other (Explain) _____

Appendix E. Incident Response Glossary

This section lists common incident response terms and definitions as they appear in Appendix D of the NIST Computer Security Incident Handling Guide.

Agent: A program used in distributed denial of service (DDOS) attacks that sends malicious traffic to hosts based on the instructions of a handler.

Baselining: Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.

Blended Attack: Malicious code that uses multiple methods to spread.

Boot Sector Virus: A virus that plants itself in a system's boot sector and infects the master boot record.

Computer Forensics: The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Computer Security Incident: See "incident."

Computer Security Incident Response Team (CSIRT): A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).

Denial of Service (DoS): An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.

Distributed Denial of Service (DDoS): A DoS technique that uses numerous hosts to perform the attack.

Egress Filtering: The process of blocking outgoing packets that use obviously false Internet Protocol (IP) addresses, such as source addresses from internal networks.

Event: Any observable occurrence in a network or system.

False Positive: An alert that incorrectly indicates that malicious activity is occurring.

File Infector Virus: A virus that attaches itself to a program file, such as a word processor, spreadsheet application, or game.

File Integrity Checker: Software that generates, stores, and compares message digests for files to detect changes to the files.

Forensics: See "computer forensics."

Handler: A type of program used in DDOS attacks to control agents distributed throughout a network. Also refers to an incident handler, which refers to a person who performs incident response work.

Honeypot: A host that is designed to collect data on suspicious activity and has no authorized users other than its administrators.

Inappropriate Usage: A violation of acceptable computing use policies.

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident Handling: The mitigation of violations of security policies and recommended practices.

Incident Response: See "incident handling."

Indication: A sign that an incident may have occurred or may be currently occurring.

Ingress Filtering: The process of blocking incoming packets that use obviously false IP addresses, such as reserved source addresses.

Intrusion Detection System (IDS): Software that looks for suspicious activity and alerts administrators.

Macro Virus: A virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate.

Malicious Code: A virus, worm, Trojan horse, or other code-based entity that infects a host.

Message Digest: A cryptographic checksum, typically generated for a file that can be used to detect changes to the file; Secure Hash Algorithm-1 (SHA-1) is an example of a message digest algorithm.

Mobile Code: Software that is transmitted from a remote system to a local system, then executed on the local system without the user's explicit instruction; examples of mobile code software are Java, JavaScript, VBScript, and ActiveX.

Multiple Component Incident: A single incident that encompasses two or more incidents.

Packet Sniffer: Software that observes and records network traffic.

Patch Management: The process of acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization.

Port Scanning: Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).

Precursor: A sign that an attacker may be preparing to cause an incident.

Profiling: Measuring the characteristics of expected activity so that changes to it can be more easily identified.

Risk: The probability that one or more adverse events will occur.

Rootkit: A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.

Scanning: Sending packets or requests to another system to gain information to be used in a subsequent
attack.

Signature: A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

Social Engineering: An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Threat: The potential source of an adverse event.

Trojan Horse: A non self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose.

Unauthorized Access: A person gains logical or physical access without permission to a network, system, application, data, or other resource.

Victim: A machine that is attacked.

Virus: A self-replicating program that runs and spreads by modifying other programs or files.

Virus Hoax: An urgent warning message about a nonexistent virus.

Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.

Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Source: NIST Special Publication 800-61: *Computer Security Incident Handling Guide*, http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

Appendix F. Incidents and Suspicious Events

Description	Reporting Party	Category
A virus/worm email hoax	System Users	Malicious Code
Attempts to "Social Engineer" or otherwise convince users/administrators to provide information to unauthorized parties	System Users	Other
Unexplained modification or deletion of data	System Users	Unauthorized Access
Denial/disruption of service or inability of one or more users to log in to an account	System Users	Unauthorized Access
User account that has been compromised	System Users	Unauthorized Access
Misuse of system resources by valid users	System Users	Unauthorized Access
Multiple unsuccessful logon attempts	System Users	Unauthorized Access
Unexplained attempts to write to system files or changes in system files	System Users	Unauthorized Access, Malicious Code
Unusual usage patterns	System Users	Unauthorized Access, Malicious Code
Operation of an unauthorized program or sniffer device to capture network traffic	System Support Staff	Probes and Reconnaissance Scans
Unauthorized vulnerability scanning	System Support Staff	Probes and Reconnaissance Scans
Unauthorized port scanning	System Support Staff	Probes and Reconnaissance Scans
Priority system alarm or similar indication from an intrusion detection tool and it has been confirmed that it is NOT a false positive	System Support Staff	Probes and Reconnaissance Scans, Malicious Code, Denial of Service (DOS)
Suspicious entries in system or network accounting (e.g., a UNIX user obtains root access without going through the normal sequence)	System Support Staff	Unauthorized Access
Accounting discrepancies (e.g., someone notices a 45-minute gap in the accounting log in which no entries whatsoever appear)	System Support Staff	Unauthorized Access
Unexplained new user accounts	System Support Staff	Unauthorized Access
Unusual time of usage (many computer security incidents occur during non-working hours)	System Support Staff	Unauthorized Access
An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user	System Support Staff	Unauthorized Access
Unexplained new files or unfamiliar file names	System Support Staff	Unauthorized Access
Unexplained modifications to file lengths and/or dates, especially in system executable files	System Support Staff	Unauthorized Access, Malicious Code

Appendix G. EDCIRC Incident Response Coordinator Procedures

Security is a growing concern. Despite the many technological advances to counteract security violations there continue to be security violations and incidents. Effectively tracking and monitoring these security violations enables management to make informed decisions pertaining to policies, programs, and allocation of resources. These decisions can then be successfully used to minimize the impact from the current incident and similar incidents in the future.

Definition

The Department has adopted the NIST Special Publication 800-61 definition of a computer security incident: "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." Typically, the incident response life cycle consists of six stages:

(1) Preparation: Establish an approach to incident response, to include defining incidents, developing policy and procedures, and identifying and implementing other components required for responses.

(2) Detection/Identification: Analyze detection components (e.g., intrusion detection systems, firewalls, audit logs) to identify signs of an incident and verify that an incident has occurred, notify appropriate officials, and safeguard evidence to ensure a verifiable chain of custody.

(3) Containment: Stop the incident before it spreads or causes more damage.

(4) Eradication: Identify and mitigate the cause of the incident (e.g., un-patched system) and components of the incident (e.g., malicious code).

(5) Recovery: Restore affected systems to an unaffected state and validate them in terms of functionality and security.

(6) Follow-up: Develop follow-up reports; extract lessons learned for the Incident Management Program, and update policies, procedures, and other elements as necessary.

Everyone has a role and associated responsibilities within the incident response life cycle. The Department of Education's Computer Incident Response Capability (EDCIRC) is a function of the Office of the Chief Information Office (OCIO) Information Assurance Services (IAS) office. The EDCIRC Coordinator serves as the primary focal point, Department-wide, for incident reporting and escalation activities. In an incident response and handling effort, the Incident Handler ensures that response and handling procedures are followed while the Incident Coordinator is responsible for the reporting and escalation activities. These escalation activities involve determining whether or not the incident should be reported to the Department's Office of Inspector General's Computer Crimes Unit (OIG/CCU) and/or to US-CERT.

Incidents Reportable to the OIG

Incidents that may constitute a computer crime (violations of applicable Federal and/or State laws) must be reported to the OIG. These incidents may include, but are not limited to, the following:

§ Compromise of systems privileges (root access);

§ Compromise of information protected by law (note that in the event of a compromise whether actual or suspected that this information must be submitted to US-CERT within one hour of identification of the incident);

§ Unauthorized access of Department IT systems and/or databases;

§ Denial of service of major IT resources;

§ Child pornography; and

§ Malicious destruction or modification of Department data and/or information (website defacement).

CCU cannot investigate a computer security incident without receiving a timely incident reports. The failure to provide OIG timely incident reports may directly impede the criminal investigative activities of the CCI staff. The Department may lose information that is vital to our securing of evidence, as well as, making important connections to ongoing cases and making decisions about initiating new cases, if incidents are not reported as soon as possible.

Incidents Reportable to US-Cert

According to http://www.uscert.gov, the types of activities that may be reportable to US-Cert include, but are not limited to, the following:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- The unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Loss or suspected loss of Personally Identifiable Information (PII) in physical or electronic form (this must be reported to US-CERT within one hour of first discovery)

Reporting an incident to US-Cert involves directing a browser to http://www.uscert.gov and clicking on the “Report an Incident” button. By completing the series of questions on the next few pages allows one to complete the reporting of an incident to US-Cert.

Non-reportable Incidents

Not every event that fits the definitions above needs to be reported. For example, the computer systems at the Department of Education are attacked daily by routine attempts to send viruses into the system, and these are effectively managed by key countermeasures. Other events include, but are not limited to, routine probes, port scans, or other common events. Such expected and unsuccessful incidents do not need to be reported to the OIG or to US-Cert. However, they should be recorded as described below.

Entering Data

PIP Portal

There are two main types of data to insert into the PIP Portal. The first type of data is the routine incident data. One example of routine data that is entered into the PIP Portal is the weekly virus reports. After logging into the PIP Portal, the weekly virus reports are inserted into the PIP Portal by clicking on the Incident Management link on the PIP Portal menu. On the Incident Management Dashboard screen scroll to the bottom of the page and click on the "Add/Edit" button. On the Incident Status screen scroll to the bottom of the page and click on "Add New Incident" button. On the Incident Profile screen the following fields need to be updated:

- Date of Incident (Date data is being inserted)
- Reported by (Person who provided the virus information)
- Date Reported (Date data was being reported)
- POC Assigned (Jerry Davis)
- System (EDNet)
- Incident Category (Cyber)
- Incident Type (Malicious Code)
- Status (Closed)

The virus information then gets inserted into the summary of incident form according to a specific format. An example of the format as it gets entered is listed below.

Weekly Virus Report Monday, April 11, 2005

2005-04-04
Heat Ticket: 01336998 virus
Heat Ticket: 01337011 virus

2005-04-05
Heat Ticket: 01337572 virus

2005-04-06
Heat Ticket: 01338258 virus
Heat Ticket: 01338381 virus

2005-04-07
Heat Ticket: 01338825 virus
Heat Ticket: 01338834 virus

2005-04-08
Heat Ticket: 01339470 virus

GRAND TOTAL: 14

The other types of reports that are inserted into the PIP Portal are incidents that are reportable to either the OIG or to US-Cert. These incidents are also entered on the Incident Profile screen described above but they also require that one fill out additional items on the screen as necessary. This includes, but is not limited to, "Incident Reported to", "FedCirc Report #", and "Affected Agency". "Summary of Incident" and "Comment" should also be well documented.

Spreadsheet collection

The spreadsheet is found at K:\OCIO\Information Assurance\Operations_Incident Response_IR Tracking\2005 (or the appropriate year). The spreadsheet is named "Incident Report Tracking Log 2005.xls". To fill out the spreadsheet fill each of the columns with the appropriate data. Adding one to the first four numbers of the row before the one you are working on and appending the date of the incident to it derives the current "Incident Report" column number. Note that the "Incident Report" and "Status of Incident" columns are hyperlinked to more information about the incident.

In the case of the weekly virus report the "Incident Report" and "Status of Incident" columns are hyperlinked to a copy of the weekly virus report that is copied into the "K:\OCIO\Information Assurance\Operations_Incident Response_IR Tracking\2005\Computer\Weekly Virus Reports" folder. In this case also the "Weekly Virus Tracking" tab in the worksheet must be filled out. In this tab the "Report Number" column is the "Incident Report" number from the "Incident Tracking" tab. Note that this number is also hyperlinked to the weekly virus report. The "Total Hosts Infected" column is the number from the "Grand Total" from the weekly virus counts file.

Emergency Escalation

The EDCIRC Coordinator will undertake the following actions as needed:
- Establish the management "war room" in the office of the Chief Information Security Officer
- Establish a teleconferencing bridge for use by OCIO senior management
- Receive periodic updates from Incident Coordinators on the status of incident response
- Keep OCIO senior management informed of the status of incident response
- Identify if and when the OIG or other law enforcement should be brought into an incident investigation.

Appendix H. References

Computer Security Act	Computer Security Act of 1987, P.L. 100-235, as amended by P.L. 104-106
IA Security Policy	Department's Handbook for Information Assurance Security Policy (http://wdcrobiis08/doc_img/acs_hb_ocio_1.doc)
Departmental Directive	The Privacy Act of 1974 (The Collection, Use, and Protection of Personally Identifiable Information)
Privacy Act	Privacy Act of 1974, 5 U.S.C. § 552a
FISMA	Title III of the E-Government Act of 2002, the Federal Information Security Management Act (FISMA), P.L. 107-347
NIST SP 800-61	NIST Special Publication 800-61: Computer Security Incident Handling Guide. (http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf)
OMB A-130	Office of Management and Budget (OMB) Management of Federal Information Resources Circular A-130, Appendix III, November 28, 2000 (http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)
OMB M-06-19	Office of Management and Budget (OMB) M-06-19: Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments (http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-19.pdf)