Standard RS.CO: Computer Crime Incident Reporting

January 13, 2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.01.15 12:37:29 -05'00'

Steven Hernandez
IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
1.0	04/19/2019	Initial draft
1.1	08/12/2019	Revised actionable incidents list 2.1
1.2	12/15/2019	Underwent annual policy review for accuracy and timeliness and to incorporate updates to NIST SP 800-53 Rev. 4. No updates were required as of December 2019.
2.0	1/22/2020	Major review and revisions on entire document
2.1	2/12/2020	CISO review and update
2.2	1/13/2021	Updates to remediate FISMA Audit deficiencies, including updates to consolidate previous sections 1.3 and 2.1 into table format, and additional clarification for OIG/TCD reportable events.

Table of Contents

1 INTRODUCTION

1.1 Purpose

This document establishes standards for reporting potential cyber security crimes within the Department of Education (ED) to the appropriate parties. In doing so, it supersedes any prior documentation establishing such standards. The standards established in this document derive authority from the Department's overarching cyber security policy, OCIO 3-112.

1.2 Scope

The standards established in this document apply to all employees, contractors, and users authorized to access ED information systems.

1.3 Background

This document details the processes necessary to ensure that the Office of Inspector General (OIG), Technology Crimes Division (TCD), has the necessary information and cyber artifacts to execute their mission responsibilities.

The OIG is the principal law enforcement agency responsible for the investigation of potential criminal and civil violations of federal law as they relate to the Department's programs and operations.

The OIG component responsible for investigating technology-related crimes is the TCD, which falls under the Assistant Inspector General for Information Technology Audits and Computer Crime Investigations (ITACCI). The TCD performs cyber-criminal investigations in response to attacks against, and unauthorized access of, Department information systems networks, databases, and computer communications systems.

2 STANDARD

2.1 OIG Reportable Events

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:

Reportable Events to OIG

Description	Example
Denial of Service (DoS)	CISA reports of DoS attacks on ED systems. Examples of DoS include, Buffer Overflow, ICMP Floor, and SYN Flood attempts.
Unauthorized Access on internally and externally hosted systems, as well as FSA partner systems	Individuals intentionally trying to gain access to PII information, systems, or components that they do not authorization to access.
Exceeding authorized access (abuse of system privileges)	A system user uses his or her privileges to conduct unauthorized searches for loan information.
Criminal misuse of information technology (IT) resources	An employee who uses his or her government issued equipment to operate a business on government time and government laptop. Additional activities include, fraud, theft, hacking, and identify theft.
Illegal interception of electronic communications	An individual who set themselves up as proxy or delegate to get access to an executive's email account without their knowledge. The use of any electronic, mechanical, or other device to intercept communications transmitted by wire, cable, or radio, e.g. Man-in-the-Middle, unauthorized port mirroring/packet capture, and unauthorized proxies or Wi-Fi hotspots with the intention of intercepting end-user traffic.
Compromise of System or Application privileges (root access)	An external threat actor compromises an admin/root account on a system or application.
Compromise of information protected by law	During contract negotiations, a Department employee or contractor sends non-releasable contract or bid related information to their private, or their company, email address. When an employee's misconduct or administrative investigation (involving one or more employees) is being reviewed by management, and an individual then releases that information to the press or media without authorization.

Attempts to access child pornography	An individual is found to be accessing child pornography using Department systems.
Malicious destruction or modification of Department data and/or information	An example is when an individual is found to be maliciously deleting or modifying Department data without proper authorization, including Department data hosted at external partner systems (e.g. Servicers, Title IVs, and Schools).

Non-Reportable Events to OIG

Unauthorized Disclosure	A user accidentally sends an email of another individual's SSN to the wrong email address. The user then self-reports the event to EDSOC. A user self-reports finding an unprotected document, configured without the proper security permissions, containing PII, such as Social Security numbers. The user informs EDSOC of his or her discovery. EDSOC conducts a review and determines only authorized users have access to the file.

If a questionable event takes place that is not identified in either of the tables above, verbally contact TCD for guidance.

3 ROLES AND RESPONSIBILITIES

3.1 EDSOC Coordinator

The EDSOC Coordinator is responsible for coordinating all reportable events with the appropriate OIG personnel. The EDSOC Coordinator is responsible for tracking and reporting on adverse event activities to include any after action reports associated with incidents. The report will include actions taken, overall impact of the event, direct and indirect costs associated with the incident response and the associated remediation actions.

3.2 ED Security Operations Center (EDSOC)

The EDSOC provides 24x7x365 surveillance, situational monitoring, and cyber defense services to rapidly detect and identify malicious activity and promptly subvert that activity. The EDSOC also collects data and maintains metrics that demonstrate the impact of the Department's cyber defense approach, its cyber state and cyber security posture. The

EDSOC operates under the Branch Chief of Cyber Operations who directly reports to the Chief Information Security Officer (CISO).

3.3 OIG Technology Crimes Division (OIG TCD)

The TCD performs cyber-criminal investigations in response to attacks against and unauthorized access of ED's information systems networks, databases, and computer communications systems. The TCD also investigates the criminal misuse of ED computers, which could include the accessing of child pornography. In addition to conducting criminal investigations, the TCD performs forensic analysis of computer media in support of criminal investigations.

3.4 Criminal Violations

Any employee with information regarding a possible criminal violation by an employee or program participant (e.g., contractor, subcontractor, grantee, subgrantee, or consultant) must bring this information to the immediate attention of the nearest OIG/Investigation Services (IS) office, the Technology Crimes Division, or the OIG Hotline. The types of computer crime incidents that must be reported are identified in the **Department of Education Incident Reporting Guidelines**.

4 COORDINATION PROCESS

4.1 Incident Response Handling

The Department follows the Incident Response Lifecycle process outlined in *NIST SP 800-61 Rev 2* (or latest version), *Computer Security Incident Handling Guide, Aug 2012*. This Standard concentrates on the OIG involvement in the last three steps of the incident management lifecycle.

Based on indicators and information received, the initial Incident Handler (EDSOC) will initiate the Incident Handler procedures. 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 Standard Operating Procedures (SOPs) are followed.

The EDSOC Coordinator shall serve as the primary focal point, Department-wide, for incident reporting and escalation activities. The EDSOC Coordinator is responsible for reporting and escalation activities and for coordinating actions with the OIG TCD, which in turn determines the appropriate law enforcement requirements and may provide additional investigative and forensic capabilities.

4.2 Detection and Analysis

During the **Detection and Analysis** stage, the Incident Handler and EDSOC 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 EDSOC 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 ED. Depending on the threat and severity of the incident, it may be necessary to involve additional personnel to determine the scope of the threat.

- **Scope Determination**: Once it is determined that a threat requires a response, the scope is determined relative to its overall impact to ED's mission and functions. Other factors that are a part of the process of determining the scope include how many systems are impacted and affected users.

The initial response procedures include:

- **EDSOC**:
    - 1. Establish a teleconferencing bridge for incident use
    - 2. Report to Cybersecurity and Infrastructure Security Agency (CISA)
    - 3. Provide updates as necessary to EDSOC Coordinator
- **EDSOC**: Receive periodic updates from Incident Handler(s), System Owners, and/or Subject Matter Experts (SMEs) on the status of incident response
- **EDSOC Coordinator**: Identify if/when the OIG should be brought into an incident and initiate contact with the Duty Agent

The EDSOC Coordinator ensures that the OIG Duty Agent is immediately notified via telephone of all incidents containing criminal or civil violations following the **Department of Education Incident Reporting Guidelines**, as well as other high visibility or on-going incidents containing criminal or civil violations. Follow-on reporting will be via email, unless directed otherwise.

4.3 Containment, Eradication, and Recovery

4.3.1 Containment

Containment is the process of stopping the incident from spreading or causing more damage. To prevent any damage to evidence, containment activities should be coordinated with the EDSOC Coordinator, who will consult with the OIG TCD. If the incident might result in a future investigation by OIG TCD, the Incident Handler needs

to take all actions to preserve the status of the system according to directions provided by the EDSOC Coordinator after consultation with the OIG TCD.

4.3.2 Eradication

Eradication is the process of identifying the cause of the incident and mitigating that cause, as well as removing components of an incident. Eradication may destroy evidence of the incident and the OIG TCD must be involved. Each step of the eradication process needs to be documented just in case the system needs to be restored. All documentation will be included in the case file within the SecOps ticketing system and provided to the EDSOC Coordinator to report to the CISO.

ED Contactor Security Personnel will then evaluate the scans and steps involved to ensure that the threat has been mitigated. They will then prepare and submit the Incident Report Summary which will include the Root Cause Analysis (RCA) to the CISO, Branch Chief of Cyber Security, and the EDSOC Coordinator. The EDSOC Coordinator will then submit the Incident Report Summary to the OIG and share the results with the System Owner.

4.3.3 Recovery

In the course of the containment actions, a determination will need to be made about whether or not the evidence will need to be preserved. In the event that evidence needs to be preserved, the EDSOC Coordinator will coordinate with OIG and the System Owner for next steps. In the event that evidence does not need to be secured, it will need to be determined whether or not the system will need to be restored for full service. If there is no need to restore service, or after service has been restored, the machine will be returned to the System Owner.

4.4 Post Incident Activity

The appropriate documentation and reporting will be accomplished to include transfer of evidence, via a Chain of Custody, to close out the incident. The Chain of Custody shows who took what actions and when, including clearly documenting each transfer of evidence (e.g., date, time, persons involved). This is especially important in preserving any physical or digital evidence that may be analyzed by the OIG TCD. Furthermore, when digital evidence is received, it should be hashed so the integrity of the data can later be verified.

Any analysis will be made on copies of the original data. No changes should be made to any physical or digital evidence. Preservation of evidence is a vital element of the incident response process and failure to properly collect, track, and maintain may result in lost data that would assist in the full remediation of incidents.

5 REPORTS

The EDSOC Coordinator, through the EDSOC, will maintain incident metrics that provide historical trends and track ED's response actions. The metrics serve as the basis for periodic reports to the OIG.

5.1 Monthly Report

The EDSOC Coordinator will provide a copy of the Incident Handling monthly report to OIG TCD. The ED monthly incident report will assist OIG TCD in reporting to other law enforcement agencies as needed. The monthly report includes the trend metrics for the month.

The report will be distributed by the 5th of each month (or the first workday after the 5th for weekends and holidays) via email with all sensitive information encrypted in a zip file using a prearranged password or using PIV encryption. ED will leverage support from law enforcement in prosecuting those that would harm the Department. In addition, OIG will have Ad Hoc access to all incident data via the SecOps ticket system.

6 APPENDIX A: GLOSSARY

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 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).

Controlled Unclassified Information (CUI): A category of information managed by the Department that is not considered vital to the national security, but the indiscriminate disclosure of which would result in the degradation or loss of public confidence. This information may be found to contain the label **For Official Use Only** or **For Internal Use Only** or **Privacy Act Protected information**, but it is still considered CUI. Due diligence is required to protect this category of information.

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.

ED Security Operations Center (EDSOC) Coordinator: Individual tasked with coordinating incident response activities across ED.

ED Security Operations Center (EDSOC): A 24x7 hour capability set up for the purpose of managing, monitoring, and responding to cybersecurity events and incidents.

Event: Any observable occurrence in a network or system.

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.

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

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

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

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 set of keystrokes used to gain unauthorized access to a system.

7 APPENDIX B: ACRONYMS

ACS	Administrative Communications System
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COR	Contracting Officer Representative
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DNS	Domain Name Service
DoS	Denial of Service
ED	Department of Education
EDSOC	Department of Education Security Operations Center
FSA	Federal Student Aid
IA	Information Assurance
IAS	Information Assurance Services
IG	Inspector General
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OIG/TCD	Office of Inspector General/Technology Crimes Division
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POC	Point of Contact
RCA	Root Cause Analysis
SAOP	Senior Agency Official for Privacy
SecOps	Incident Handling Case Management Tool
SER	Suspicious Event Report
SP	Special Publication
TCD	Technology Crimes Division
US-CERT	United States Computer Emergency Readiness Team