



F E D E R A L  
S T U D E N T A I D

*We Help Put America Through School*

---

# **- Incident Response Training - Handling and Reporting Incidents at FSA**

---

**June 19, 2003**

---

*"We help put America through school"*



# Introduction

---

Who is impacted by this training?

- System Security Officers
- Contractors operating your systems
- Contracting Officers if changes need to be made

How is this training different from what the Department offers?

- Department's training is more of an overview of Incident Response
- FSA training will explain how FSA will implement the Department's Incident Response guidance.

# Topics

---



1. Department's Incident Response Program
  - Why have a Computer Incident Response Program?
  - Defining Security Incidents and Suspicious Activity
2. FSA's Implementation of the Department's Program
  - Review of the *FSA Security Incident Implementation Guide*
3. Reporting Security Incidents and Suspicious Activity

# Why Incident Response?

---



**It happens in the Cyber-world too! How will you respond?**



# Security Incident or Suspicious Activity?

A Security Incident is any event that has resulted in:

- unauthorized access to, or disclosure of, sensitive information;
- unauthorized modification or destruction of system data;
- reduced, interrupted, or terminated data processing capability;
- introduction of malicious program or virus activity; or
- the degradation or loss of the systems Confidentiality, Integrity or Availability; or the loss, theft, damage, or destruction of an IT resource.

Suspicious Activity is any activity that is considered:

- an abnormal system event occurrence for a given system that cannot be immediately explained, but does not pose an immediate threat;
- observed recurring activity that possibly indicates attempts are being made to exploit a vulnerability but is countered by security controls in place;
- sporadic repeated activity that cannot be readily explained by system operations and security staff;
- activity that, when combined with other factors or anomalous events, **indicates a possible cause for concern.**

Identifying security incidents and suspicious activity requires familiarity with the system and acceptable system thresholds.



# Department's Incident Handling Program

---

OCIO operates a central incident handling capability to assist ED systems respond to incidents and limit an incident's impact on the Department.

- Department of Education Computer Incident Response Capability (EDCIRC).
- Established initial operating capability in 2002
- Supported full-time by ED staff and a contractor
- Incident Handling procedures contained in Department's *Incident Handling Guide*



# FSA Implementation

---

## Three steps to success:

- **Step One: Report all Security Incidents, which is not a new requirement.**
- **Step Two: Establish reporting for Suspicious Activity. Establish monitoring and log review standards. May require modifications to current practices.**
- **Step Three: Analyze and assess costs for an FSA-based Incident Response team and/or center (forward looking).**

**Time Frame for Implementation? Starting today!**



# Overview of the FSA Guide

The FSA guide provides the specific reporting procedures FSA system personnel need to follow.

	<b>1.0 INTRODUCTION .....</b>	<b>3</b>
	1.1 Purpose.....	3
	1.2 Scope.....	3
	1.3 Document Structure .....	3
→	1.4 Definitions.....	4
→	<b>2.0 MONITORING SYSTEMS, KEEPING AND REVIEWING LOGS .....</b>	<b>6</b>
	2.1 Security Incident VS. Suspicious Activity.....	6
→	<b>3.0 REPORTING SECURITY INCIDENTS .....</b>	<b>7</b>
→	3.0 Table – Security Incident Handling Process .....	7
	3.1 FSA Security Incident Reporting Action Chain .....	8
→	3.2 Diagram - FSA Security Incident Reporting Chain .....	9
→	3.3 Table – Security Incident Reporting Chain, Timeline Summary .....	10
	3.4 What to expect and do after the report.....	10
	3.5 Preservation of Evidence .....	10
	3.6 Alternate Connectivity .....	10
	3.7 Three-way Consulting.....	11
	3.8 Final Status.....	11
→	<b>4.0 REPORTING SUSPICIOUS ACTIVITY .....</b>	<b>12</b>
→	4.0 Table - Suspicious Activity Handling Process.....	12
	4.1 ‘Suspicious or Anomalous Activity’ Action Chain .....	13
→	4.2 Diagram - FSA Suspicious Activity Reporting Chain.....	14
→	4.3 Table – Suspicious Activity Reporting Chain, Timeline Summary .....	14
	4.4 What to expect and do after the report.....	15
→	<b>APPENDIX A - FSA SECURITY INCIDENT CONTACT LIST .....</b>	<b>16</b>



# The Suspicious Event Report (top)

US Department of Education Computer Security Suspicious Event 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					
<b>Name</b>		<b>Title</b>		<b>Organization</b>	
<b>Address</b>					
<b>Phone</b>		<b>Fax</b>		<b>E-mail</b>	
Location Information					
<b>Building number</b>		<b>Room Number</b>		<b>Rack/Cube Location</b>	
Time Information					
<b>Date</b>		<b>Time</b>		<b>Time Zone</b>	
Classification of the Suspicious Activity					
	<b>Denial of Service</b>		Web Site Defacement		Social Engineering
	<b>Virus / Malicious Code</b>		User Account Compromise		Hoax
	<b>System Misuse</b>		Other Intrusion		Network Scanning/Probing
	<b>Technical Vulnerability</b>		Root Compromise		Other/Specify:
<p><b>If a Virus</b>, 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:</p>					
<p><b>If a Technical Vulnerability</b>, 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:</p>					



# Suspicious Event Report (bottom)

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			
<b>Incident Assessment:</b> 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							
<b>Actions Taken:</b> (1) What actions have been taken on the system (Back-ups, commands, removed from network, etc). (2) Who has been notified?							
<b>Additional Information:</b> (If this incident is related to a previously reported incident, include any previously assigned incident number for reference.):							



# Reporting Security Incidents (1)

## 3.0 REPORTING SECURITY INCIDENTS

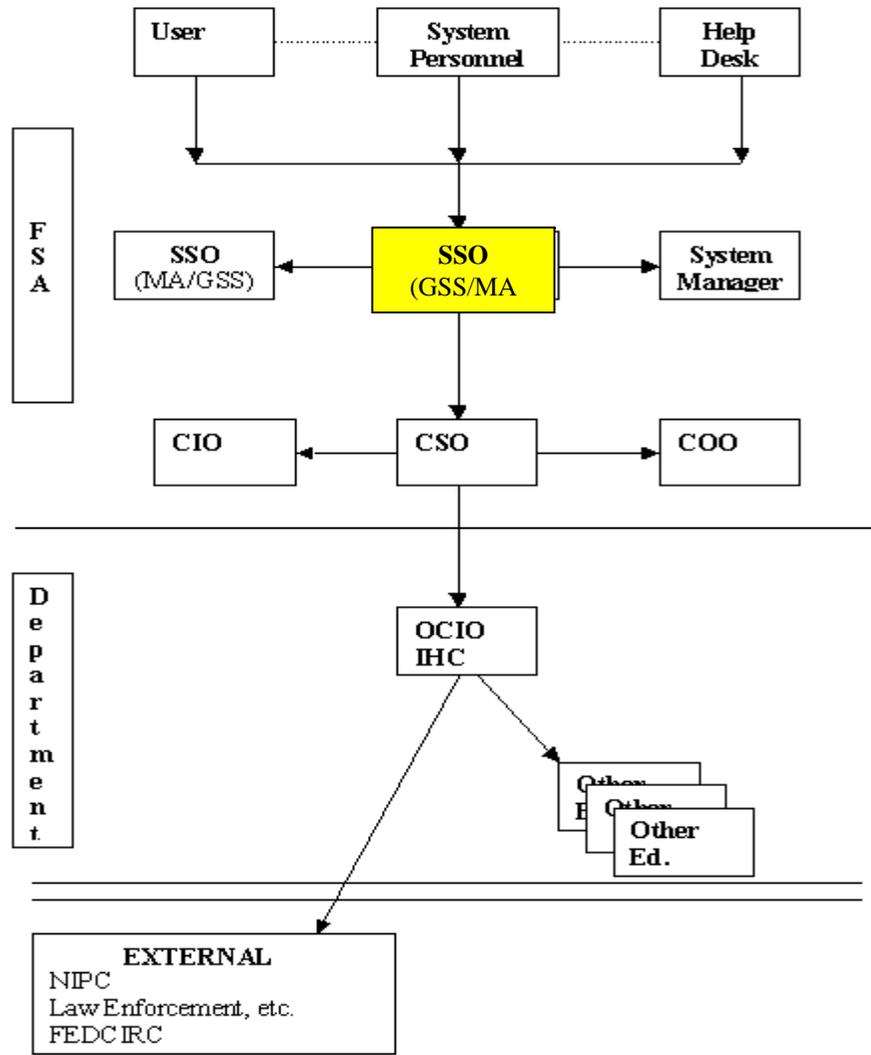
The following table provides a concise view of what actions stakeholders should take in response to security incidents. The activities are presented chronologically starting with row one (1). Note rows 8, and 11 actions start in the EDCIRC column.

**3.0 Table – Security Incident Handling Process**

Contractors	FSA	Ed or EDCIRC
1) Monitor and Review systems and logs		
2) Security Incident identified		
3) Immediately notify FSA for authority to take system off-line	3a) Approve System to go off-line and notify EDCIRC of decision	
4) If instructed, take system off-line, isolate and freeze.		
5) Complete incident form and follow reporting chain. (See Diagram 3.2)	5a) SSO reviews Report relays it to CSO, CSO to EDCIRC	5b) EDCIRC reviews report – Provides feedback and “next-step” information. Notifies FEDCIRC and others as necessary.
6) Follow instruction from EDCIRC	6a) Follow instruction from EDCIRC	
7) Provide status on actions taken	7a) Receive contractor status	7b) Receive contractor status
		S T A T U S
9) Propose alternate/backup system Wait for approval	9a) Receive alt. request- Approve	
10) Implement alt. system		
11b) Receive Findings Report Consult on course of action.	11a) Receive Findings Report Consult on course of action	11) Analysis complete and findings submitted. Course of action proposed.
12) Course of action followed and completed.		
13) Security Incident resolved Request system reestablishment Wait for approval.	13a) System re-establishment approved.	
14) Lessons Learned		

# Reporting Security Incidents (2)

3.2 Diagram - FSA Security Incident Reporting Chain





# Reporting Security Incidents (3)

- The response times are mandatory and represent maximum time limits.
- If you cannot reach the next in the chain, do not wait, skip that person and contact the following person in the chain.

**3.3 Table – Security Incident Reporting Chain, Timeline Summary**

Position	(Reports Incident using SER form To) Position	Response Time
System Administrator	System Security Officer (SSO)	Immediately
System Security Officer (SSO)	FSA Incident Coordinator or CSO	1 hour
Computer Security Officer (CSO)	Dept. OCIO Incident Handling Coordinator and PO Senior Officers	3 hours
Dept. OCIO Incident Handling Coordinator	Deputy Chief Information Officer	1 hour
Deputy Chief Information Officer	Chief Information Officer	1 hour
Chief Information Officer or CIO's Designee	Deputy Secretary, Inspector General, and others as appropriate	1 hour



# Reporting Suspicious Activity (1)

The Department has established two types of Suspicious Activity and mandatory report times.

## 4.0 REPORTING SUSPICIOUS ACTIVITY

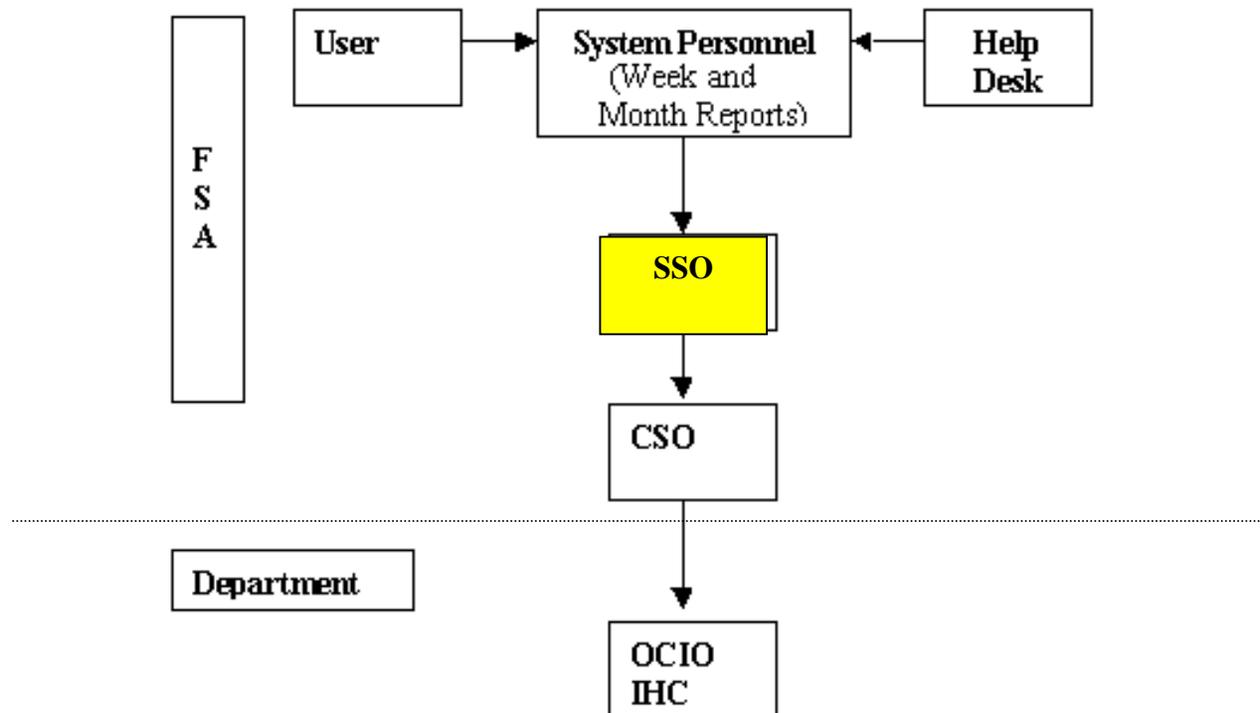
The following table provides a concise view of actions associated with reporting suspicious activity for the major stakeholders. Follow the numbers from lowest to highest to find the next expected action. Please note that on rows 5 and 6 actions start in the EDCIRC column.

**4.0 Table - Suspicious Activity Handling Process**

Contractors	FSA	Ed or EDCIRC
1) Monitor and Review systems and logs		
2) Suspicious Activity identified		
3) System left on-line		
4) -Week Report - Category A activities -Month Report - Category B activities	4a) SSO reviews Report, relays it to CSO, CSO to EDCIRC	4b) EDCIRC reviews Report
		5) Analysis of Activity 1) Allowed activity 2) Inconclusive – mark and monitor 3) Security Incident (see Chart 4)
6b) Take action as advised by EDCIRC.	6a) Receive action and feedback report from EDCIRC	6) Provides analysis feed back and required action to FSA and Contractor

# Reporting Suspicious Activity (2)

4.2 Diagram - FSA Suspicious Activity Reporting Chain





# Reporting Suspicious Activity (3)

**4.3 Table – Suspicious Activity Reporting Chain, Timeline Summary**

<b>Position</b>	<b>(Reports Incident using *SER form To) Position</b>	<b>Category A Response Time</b>	<b>Category B Response Time</b>
System Administrator	System Security Officer (SSO)	Within the Month	Within the Week
System Security Officer (SSO)	Computer Security Officer (CSO)	Within the Month	Within the Week
Computer Security Officer (CSO)	OCIO Incident Handling Coordinator	Within the Month	Within the Week
OCIO Incident Handling Coordinator	Back to originating office	24 to 48 hours	24 to 48 hours

\* SER is the Suspicious Event Report form



# What Would You Do?

---

- Security Incident
  - It is 4:30 pm on a Friday. Your system administrator calls you and tells you that there has been a web defacement...
  - You come to work on Monday. In your email is an SER telling you of a virus on your system's server. The SER was sent to you and others on Saturday. There are what appear to be follow-up messages...
- Suspicious Activity
  - Thursday afternoon you get an email with several attached SERs with reports of a high number of port scans, multiple unsuccessful logon attempts and even one attempt of "social engineering"...



# Next Steps

---

- **SSOs and contract support should attend next OCIO Incident Response Training**
- **Fill in the Security Incident Contact List that will be sent to you and return it promptly.**
- **Give contractors the Department's and FSA's IR guides and request feedback**
- **If your system will have issues complying with the ED or FSA Incident Handling guidance, schedule a meeting with Bob Ingwolson and Derek Foxley soon.**