



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

*We Help Put America Through School*

# **Security Roles and Responsibilities**

**June 2003**

## Table of Contents

1	Introduction.....	4
1.1	REFERENCES .....	4
1.2	DOCUMENT MAINTENANCE .....	4
	Computer Security Officer.....	5
	CONTINUITY OF SUPPORT (COS)/ CONTINGENCY PLANNING .....	6
	CERTIFICATION AND ACCREDITATION .....	6
	POLICY.....	6
	INCIDENT RESPONSE .....	6
	RISK ASSESSMENT .....	9
	DUTY .....	9
	TRAINING.....	11
	TESTING.....	11
	System Owner.....	11
	SOLUTION LIFE CYCLE.....	11
	CONTINUITY OF SUPPORT (COS)/ CONTINGENCY PLANNING .....	12
	CERTIFICATION AND ACCREDITATION .....	12
	CONFIGURATION MANAGEMENT.....	13
	INCIDENT RESPONSE .....	13
	RISK ASSESSMENT .....	13
	ACCOUNT ACCESS .....	14
	LOGICAL CONTROLS .....	14
	SYSTEM INTERCONNECTIONS.....	14
	System Manager.....	14
	SOLUTION LIFE CYCLE.....	15
	CONTINUITY OF SUPPORT (COS)/ CONTINGENCY PLANNING .....	15
	CERTIFICATION AND ACCREDITATION .....	17
	CONFIGURATION MANAGEMENT.....	17
	INTRUSION DETECTION .....	18
	TRAINING.....	18
	INCIDENT RESPONSE .....	18
	DATA INTEGRITY .....	19
	SYSTEM SECURITY PLAN .....	20
	PERSONNEL SECURITY .....	20
	USE OF EXTERNAL CONNECTIONS .....	21
	PRODUCTION INPUT/OUTPUT CONTROLS .....	21
	MAINTENANCE AND REPAIR .....	21
	TESTING.....	21
	PASSWORDS .....	22
	LOGICAL ACCESS CONTROLS.....	22
	PHYSICAL ACCESS CONTROLS .....	23
	DOCUMENTATION .....	24
	CONTRACTORS.....	24
	System Security Officer.....	24
	SOLUTION LIFE CYCLE.....	25
	CONTINUITY OF SUPPORT (COS)/ CONTINGENCY PLANNING .....	25

CERTIFICATION AND ACCREDITATION .....	26
CONFIGURATION MANAGEMENT.....	26
INTRUSION DETECTION .....	26
TRAINING.....	26
ACCOUNT ACCESS .....	27
INCIDENT RESPONSE .....	28
DATA INTEGRITY .....	30
SECURITY PLAN .....	31
JOB DESCRIPTIONS.....	31
DISASTER RECOVERY .....	31
PENETRATION TESTING.....	31
IDENTIFICATION AND AUTHENTICATION .....	31
PASSWORDS .....	31
REMOTE ACCESS.....	31
AUDIT TRAILS.....	31
KEYSTROKE MONITORING .....	32
RISK ASSESSMENT .....	32
WEBSITES .....	32
CONTRACTS .....	32
DOCUMENTATION .....	32
System Administrator (SA).....	33
INCIDENT RESPONSE .....	34
USERS .....	36
TRAINING.....	36
ACCOUNT ACCESS .....	36
INCIDENT RESPONSE .....	36
PHYSICAL ACCESS .....	37
PORTABLE COMPUTERS .....	38
DATA CONTROLS .....	38
INTRUSION DETECTION .....	39
SOFTWARE.....	39
PASSWORDS .....	40

## **1 INTRODUCTION**

IT systems are complex and thus require numerous policy statements and procedures to oversee them. The vast amount of guidance produced within a large organization makes adherence daunting, but not impossible if the organization can structure its policies following certain disciplines. System personnel must understand their responsibilities to achieve a cohesive overall security program. Security training and awareness courses only go so far in describing the security roles and responsibilities of an organization's users and managers.

This document is a one-stop reference manual for employees that addresses the responsibilities for the primary security-related roles; including Chief Security Officer, System Owner, System Manager, System Security Officer, System Administrator and User. It eliminates the need for an FSA employee to review a number of security documents in order to gain an understanding of their role in protecting the security of the enterprise. Each role has associated security topics and tasks for each subject. There is also a document and section reference for each item for cross-reference purposes.

### **1.1 References**

This document references existing, approved Department of Education and FSA policies and procedures. The documents referenced include:

- FSA System Security Process Guide, V 3.0, March 2003
- Department of Education IT Security SDLC Security Integration Guide, V 3.2, November 2002
- FSA Information Technology Security and Privacy Policy, V 2.0, April 2003
- Department of Education Certification and Accreditation Guide, V 6.0, July 2002
- FSA Privacy Impact Assessment and Privacy Notice for Websites
- Department of Education Information Technology Configuration Management Plan Procedures, V 3.1, 2002
- Department of Education Information Technology Information Technology Contingency Planning Procedures, February 2003
- Department of Education Information Technology Security Policy, October 2001
- Department of Education Information Technology Security Program Management Plan, V 5.10, April 2003
- Department of Education Information Technology Risk Assessment Guide, V 6.2, July 31, 2002
- Department of Education Information Technology Information Security Incident Handling Procedures, V 7.1, April 2003
- FSA Memorandum of Understanding, V 1.0, June 2003

### **1.2 Document Maintenance**

FSA and the Department create new security documents and update existing security documents frequently. As FSA or the Department creates new roles and responsibilities, FSA will update this document as necessary. No less than annually, FSA will review the roles and responsibilities contained within this document and make updates as necessary.

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
<b>COMPUTER SECURITY OFFICER</b>				

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
<b>Continuity of Support (COS)/ Contingency Planning</b>		Review and approve the Continuity of Support Plan and apprise the System Owner of updated versions.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Plan Maintenance
		Ensuring compliance with the requirements for continuity of operations planning for each IT installation and resource within his or her PO.	ED Information Technology Security Policy, October 2001	Computer Security Officers
<b>Certification and Accreditation</b>		Participate as a C&A team member for the systems and manages the efforts the C&A teams and activities.	ED Certification and Accreditation Guide, V 6.0, 2002; ED IT Security SDLC Security Integration Guide, V 3.0, Sept 2002	Activity 1: Identify C&A Team, Table 1. C&A Roles and Responsibilities
		Take the PO lead in the implementation of the Department's IT security certification and accreditation (C&A) process.	ED Information Technology Security Policy, October 2001	Computer Security Officers
		Based on the documented results of the design reviews and system tests, certify that the system meets all applicable Government-wide and Department policies, regulations, and standards for certification and that the test results demonstrate that the specified security safeguards are in place and adequate.	ED Information Technology Security Policy, October 2001	System Certification and Accreditation
		Along with the system manager, unconditionally certify, conditionally certify, or refuse certification.	ED Information Technology Security Policy, October 2001	Computer Security Officers
<b>Policy</b>		Grant waivers when appropriate to exceptions in FSA policy. If approved, sign the written exception request.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Exceptions
<b>Incident Response</b>		Review the initial Suspicious Event Report (SER), received from the SSO, and related information to determine whether a potential incident has occurred.	ED Incident Handling Procedures, V 7.1, April 2003	Appendix B- Incident Reporting and Response Guidelines
		If so, forward incident reports/ SERs received from the SSO to ED Incident Handling Coordinator in	FSA Information Technology Security and Privacy Policy, V 2.0,	Appendix B- Incident Reporting and

Topic	#	Responsibility	Document	Section
		O/CIO and to his or her Principal Office senior officer within <b>three (3) hours</b> of receiving the initial report (but after some internal analysis).	April 2003 ED Incident Handling Procedures, V 7.1, April 2003	Response Guidelines

Topic	#	Responsibility	Document	Section
		Along with the SSOs, implement incident handling procedures and maintain an adequate reporting capability.	ED Information Technology Security Program Management Plan, April 2003	Risk Management Sub-program Element – Incident Response
		On an as-needed basis, assist with and/or facilitate the resolution of incidents.	ED Incident Handling Procedures, V 7.1, April 2003	Computer Security Officer
		<p>Expected to know the following:</p> <ul style="list-style-type: none"> <li>• Department security policies for IT systems</li> <li>• Detailed knowledge of security threats</li> <li>• Capability of recognizing system anomalies and assessing the impact of threats posed by those anomalies</li> <li>• Detailed knowledge of methods used to prevent security breaches</li> <li>• Detailed knowledge of methods used to recover from security breaches</li> <li>• General technical knowledge of the systems within their POC to manage responses to a security breach</li> <li>• How to assess the overall aspects of an incident and identify IT equipment, which should be suspected of being associated with the incident.</li> <li>• Detailed knowledge of evidence protective measures regarding potential IT evidence.</li> <li>• Legal issues involved with security breaches.</li> </ul>	ED Incident Handling Procedures, V 7.1, April 2003	Computer Security Officer
		Ensure that suspicious event activity is closely monitored or expand system logging capabilities as directed by the Incident Handling Coordinator, and provide report updates, if necessary on a daily basis.	ED Incident Handling Procedures, V 7.1, April 2003	ED Incident Handling Procedures, V 7.1, April 2003

Topic	#	Responsibility	Document	Section
<b>Risk Assessment</b>		Review economic (cost benefit) analyses submitted by the PO business managers to support decisions as to the most cost-effective countermeasures to reduce security risks.	ED Information Technology Security Policy, October 2001	Mission Effectiveness
		Ensure the performance of a risk analysis for each IT installation and resource within his or her PO, as described in the <i>Risk Management Program Guide</i> .	ED Information Technology Security Policy, October 2001	Computer Security Officers
<b>Duty</b>		Manage the FSA security and privacy program and actively supports the business channels in the development and maintenance of systems worthy of trust.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Roles and Responsibilities
		Serving as the primary point of contact and coordination within the PO for all IT security matters.	ED Information Technology Security Program Management Plan, April 2003	Computer Security Officers
		Ensure that the business manager for each system within the CSO's organization understands his or her IT security responsibilities, including all matters that address security.	ED Information Technology Security Policy, October 2001	Computer Security Officers
		Serve as liaison between the CIO or their designee and PO personnel responsible for system security activities.	ED Information Technology Security Policy, October 2001	Computer Security Officers
		Support all levels of management within his or her PO in required IT security planning and budgeting.	ED Information Technology Security Policy, October 2001	Computer Security Officers
		Review early in the preparation stage all IT procurements originating from their PO to ensure that IT security is incorporated into the lifecycle of the procurement and maintenance of the product or service.	ED Information Technology Security Policy, October 2001	Computer Security Officers
		Monitor, evaluate, and report annually to the CIO or his/her designee the status of the security program within his or her organization and the adequacy of programs administered.	ED Information Technology Security Policy, October 2001	Computer Security Officers

Topic	#	Responsibility	Document	Section
		Ensure the clear establishment of all data, software, and hardware ownership within his/her organization.	ED Information Technology Security Program Management Plan, April 2003	Computer Security Officers
		Responsible for the review and comment on all IT security plans, contingency plans and disaster recovery plans for all IT systems within their PO. Ensuring that appropriate personnel are aware of the dependencies associated with critical department assets.	ED Information Technology Security Policy, October 2001	Computer Security Officers
		Ensure compliance with requirements in each of the following areas for each IT system, identified assets, and facility within his or her organization: <ul style="list-style-type: none"> <li>• Physical security</li> <li>• Personnel security</li> <li>• Administrative security</li> <li>• Computer security</li> <li>• Communications security</li> </ul>	ED Information Technology Security Policy, October 2001	Computer Security Officers
		Ensure execution of the Critical Infrastructure Plan to implement security on critical IT infrastructures within the PO.	ED Information Technology Security Policy, October 2001	Computer Security Officers
		Ensure compliance with the Department's security program for all external information-processing activities (e.g., cross-servicing, computer matching, data sharing), whether conducted by or for the government.	ED Information Technology Security Program Management Plan, April 2003	Computer Security Officers
		Assist the Network Security Officer in ensuring that the security of the Department's Education Network (EDNet) resources is maintained within their PO.	ED Information Technology Security Policy, October 2001	Computer Security Officers
		Assist the business manager and contracting officer in carrying out the security provisions of the contract and solicitation policy.	ED Information Technology Security Policy, October 2001	Computer Security Officers

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
		Maintain a current list of IT systems and facilities sponsored by his or her organization, and forwarding it and any related documentation to the CIO or his/her designee upon request.	ED Information Technology Security Policy, October 2001	Computer Security Officers
		In coordination with the appropriate contracting officer, conduct annual reviews of the contract to ensure continued compliance with security policies.	ED Information Technology Security Policy, October 2001	Contracts and Solicitations
		Along with the data owner, determine approval of the removal of portable computers with resident sensitive information.	ED Information Technology Security Policy, October 2001	Physical Security
		Review requests for authorization to use privately owned software.	ED Information Technology Security Policy, October 2001	Incident Reporting and Response
		Ensure that media are free of viruses and other malicious software before authorizing their use.	ED Information Technology Security Policy, October 2001	Incident Reporting and Response
		Participate as a member of the CSOs working group and attend monthly meetings.	ED Information Technology Security Program Management Plan, April 2003	Computer Security Officers Working Group
<b>Training</b>		Provide IT security awareness briefings throughout his or her PO.	ED Information Technology Security Policy	Computer Security Officers
<b>Testing</b>		Ensure each system will undergo independent security validation and verification testing.	ED Information Technology Security Policy	System Certification and Accreditation
<b>SYSTEM OWNER</b>				
<b>Solution Life Cycle</b>		Complete the Dept's Critical Infrastructure Protection Survey during the Definition Phase of the System Security Life Cycle.	FSA System Security Process Guide, V 3.0, March 2003	Definition Phase
		During the Support Period, analyze, with the SSO, the self-assessment review, to determine security control priorities based on weakness discovered in the assessment.	FSA System Security Process Guide, V 3.0, March 2003	Support Period

Topic	#	Responsibility	Document	Section
		During the project initiation and requirements specification phases of a new system, consider contingency requirements based on the criticality of the new system.	ED Information Technology Contingency Planning Procedures, February 2003	When Should a Plan be Developed?
		Determine the mission criticality and sensitivity of the system and document it in the GSS and MA Inventory Submission Forms.	Department of Education Certification and Accreditation Guide, V 6.0, 2002	Step 1: Determine Mission Criticality
<b>Continuity of Support (COS)/ Contingency Planning</b>		Assess and determine approval for changes to processing priorities the system for contingency planning purposes.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Contingency Planning
		Ensure that the contingency plan developed addresses all of the requirements from ED's Information Technology Contingency Planning Procedures.	ED Information Technology Contingency Planning Procedures, February 2003	Applicability
		Serve as a subteam member for contingency related issues and fully understand his or her responsibilities for contingency planning and how the system ranks in terms of priority for recovery.	ED Information Technology Contingency Planning Procedures, February 2003	Contingency Planning Coordinator
		Review/incorporate contingency planning requirements in system interconnection documents (MOU, etc).	ED Information Technology Contingency Planning Procedures, February 2003	Coordination of GSS and MA Contingency Plans
<b>Certification and Accreditation</b>		During C&A testing, along with the OCIO, determine which Tier 3 systems require penetration testing.	ED Certification and Accreditation Guide, V 6.0, 2002	Activity 2: Perform Penetration Testing
		Review the SSAA documentation and send it to the Certification Review Group.	ED Certification and Accreditation Guide, V 6.0, 2002	What are the Different Types of Certification Recommendations?

Topic	#	Responsibility	Document	Section
<b>Configuration Management</b>		<p>The system owner or other designated personnel must ensure that the following questions are answered and the information should be used as part of the change request (CR) submission:</p> <ul style="list-style-type: none"> <li>• Has the product been identified and documented?</li> <li>• Has the system documentation been updated to reflect the change?</li> <li>• Has the version number, release number, and other identifiable attributes of the configuration product been documented?</li> <li>• Has the software/hardware description been noted?</li> </ul>	ED Technology Configuration Management Plan Procedures, V 3.1, 2002	Step 1: Change Identification
<b>Incident Response</b>		Ensure the users are informed of their role in the incident response program and how they are to report potential issues to their respective system SSO.	ED Incident Handling Procedures, V 7.1, April 2003	Appendix A- OCIO Incident Handling Guidelines Memo
<b>Risk Assessment</b>		Budget for and oversee the completion of risk assessments for all Information Technology (IT) systems under his/her control.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Risk Management
		Determine the effectiveness and adequacy of risk mitigations for the system.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Risk Management
		Supervise a mission/business impact analysis, including an estimated degree of harm that could occur if corrective actions are not taken.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Risk Management
		On the basis of the impact analysis, recommend corrective or mitigating actions to bring the system to an acceptable risk level.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Risk Management
		After receiving the independent risk assessment report, prioritize each risk in the process of developing a remediation plan.	ED Information Technology Risk Assessment Guide, V 6.2, July 31, 2002	Step 4: Analyze Risk

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
		Propose an implementation schedule and milestones with cost estimates for risk mitigation.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Risk Management
		Monitor updates of a system's security plan with new procedures.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Risk Management
		Maintain a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat source, including those accepted as risk-based decisions.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Risk Management
		Determine if a change to the system is major.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Risk Management
<b>Account Access</b>		Permit and approve Group IDs only when necessary.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Identification and Authentication
		Periodically re-certify users.	ED Information Technology Risk Assessment Guide, V 6.2, July 31, 2002	Technical Controls/I&A
<b>Logical Controls</b>		Review reports regarding protocols with known vulnerabilities, such as UDP and TFTP, and determine approval for usage before implementation.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Logical Access Controls
<b>System Interconnections</b>		Authorize all Memoranda of Understanding (MOU) or Trading Partner Agreements between interconnected systems.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	System Interconnections
<b>SYSTEM MANAGER</b>				

Topic	#	Responsibility	Document	Section
<b>Solution Life Cycle</b>		Assign, in writing, a system security officer (See Appendix C System Security Process Guide for example assignment letters).	FSA System Security Process Guide, V 3.0, March 2003	Vision Phase
		Identify the roles and responsibilities of the user and developer community, including FSA employees.	FSA System Security Process Guide, V 3.0, March 2003	Definition Phase
		Review the checklists from all of the phases for completion and then sign the checklists.	FSA System Security Process Guide, V 3.0, March 2003	All Phases
<b>Continuity of Support (COS)/ Contingency Planning</b>		Review the Department's Contingency Planning Policy, found in the <i>Department of Education IT Security Policy</i> and the corresponding <i>OCIO Security Policy Guidance</i> , to determine requirements and responsibilities.	ED Information Technology Contingency Planning Procedures, February 2003	Review Department Contingency Planning Policy
		Readjust, update and approve Continuity of Support Plan and disaster recovery plans as necessary to continue their effectiveness.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Plan Maintenance
		Maintain and update the plan and supporting documentation as necessary at least annually or when significant changes to the system occur.	ED Information Technology Contingency Planning Procedures, February 2003	Plan Maintenance
		Along with the CPC, maintain a list of all personnel that have a copy of the IT Contingency Plan.	ED Information Technology Contingency Planning Procedures, February 2003	Distribution of the Plan and Version Control
		As deficiencies in the plan are identified through testing and exercises, identify and implement corrective measures and provide updates to appropriate Department personnel.	ED Information Technology Contingency Planning Procedures, February 2003	Plan Maintenance
		Ensure that the contingency plan provides security controls commensurate with the system's requirements.	ED Information Technology Contingency Planning Procedures, February 2003	How Does the Contingency Plan Feed into the C&A Process?

Topic	#	Responsibility	Document	Section
		The system manager, working closely with the business manager, is responsible for developing an IT Contingency Plan for each GSS or MA under his or her control.	ED Information Technology Contingency Planning Procedures, February 2003	Who is Responsible for Developing the IT Contingency Plan?
		The SM should act as, or appoint and oversee, a contingency planning coordinator (CPC). The CPC will be responsible for organizing subteams with system specific expertise for the contingency process.	ED Information Technology Contingency Planning Procedures, February 2003	Who is Responsible for Developing the IT Contingency Plan? (CPC)
		Determine the number and size of subteams based upon the complexity of the system, whether it is a GSS or MA, and any other system-specific criteria.	ED Information Technology Contingency Planning Procedures, February 2003	Who is Responsible for Developing the IT Contingency Plan? (CPC)
		Determine the type of contingency plan required for the system on its risk assessment and tier level.	ED Information Technology Contingency Planning Procedures, February 2003	What Type of Contingency Plan is Required for Your IT System?
		Work with the CPC to evaluate and determine the type and extent of preventive measures to take based to decrease threat risk.	ED Information Technology Contingency Planning Procedures, February 2003	Identify Preventive Controls
		Decide the type or combination of backup media types based upon system requirements.	ED Information Technology Contingency Planning Procedures, February 2003	Backup Methods
		Along with the CPC and contingency planning team, determine how long backups are required based on system-specific criteria or any federal regulations.	ED Information Technology Contingency Planning Procedures, February 2003	Retaining Backups
		Be aware of whether other organizations in nearby locations might be using the same vendor for contingency services.	ED Information Technology Contingency Planning Procedures, February 2003	Alternate Sites
		Along with the CPC, when determining which method to use for equipment replacement, incorporate the impact analysis from the BIA.	ED Information Technology Contingency Planning Procedures, February 2003	Equipment Replacement

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
		Along with the CPC and contingency planning team, determine what type of facility can adequately support the system in an emergency based upon the BIA.	ED Information Technology Contingency Planning Procedures, February 2003	Alternate Sites
		Plan for the use of a secure alternate processing site geographically removed from the primary site in the event of a disaster.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Alternate Site Capability
		Ensure that backup equipment is fully compatible, especially with regard to security controls.	ED Information Technology Contingency Planning Procedures, February 2003	Equipment Replacement
<b>Certification and Accreditation</b>		Participate in the C&A process including being a member of the C&A Team.	ED IT Security SDLC Security Integration Guide, V 3.0, Sept 2002	Phase 1: Planning
		Ensure that any security deficiencies are documented in the complete accreditation package provided to the DAA.	ED Information Technology Security Policy, October 2001	Business or Functional Managers
		Review the SSAA for content, quality, and degree of completion and make a recommendation for full accreditation, IATO, or Not to turn on.	FSA System Security Process Guide, V 3.0, March 2003	Deployment Phase
		If the system is given an IATO, formulate and submit to the DAA a corrective action plan proposing the approach to mitigate identified vulnerabilities.	ED Information Technology Security Policy, October 2001	System Certification and Accreditation
		Responsible for ensuring that the necessary steps to maintain re-certification and re-accreditation are initiated every 3 years or when changes are planned that will affect the security of the GSS or MA	ED Certification and Accreditation Guide, V 6.0, 2002	Post Accreditation
<b>Configuration Management</b>		Create a configuration management plan that describes the hardware and system software maintenance controls in place and the process by which configuration controls will be maintained for that system.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Configuration Management
		Support/enforce the configuration management	FSA Information Technology	Change Management

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
		process, including descriptions and change identification, approval, and documentation procedures.	Security and Privacy Policy, V 2.0, April 2003	
		Make recommendations on training needed to implement new configurations and controls.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Change Management
		Review the updated detailed system specifications after a change has been implemented.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Change Management
<b>Intrusion Detection</b>		Monitor the status of intrusion detection tools.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Intrusion Detection
		Routinely review intrusion detection reports after suspected incidents, and assign responsibility for incident resolution and lessons learned.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Intrusion Detection
		Conduct periodic reviews on the software and data content of the systems for which they are responsible for unapproved files, etc.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Intrusion Detection
<b>Training</b>		Monitor and document the training of information security personnel who support their systems	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Security and Privacy Awareness and Training
		Ensure that incumbents of sensitive positions attend periodic IT security training programs.	ED Information Technology Security Policy, October 2001	IT Security Awareness and Training
<b>Incident Response</b>		Review incident handling procedures and control techniques after each incident and, when necessary, modify the procedures to prevent recurrence and improve response techniques/methods.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Post Incident Activities
		Collect and secure audit trails and other tracking mechanisms for analysis and use as potential evidence.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Post Incident Activities

Topic	#	Responsibility	Document	Section
		If, during system log reviews, a suspicious event is discovered, the system administrator, SSO or system manager will categorize the event according to the Department's Schedule B – Incident Reporting & Response Guidance – Suspicious Event Matrix.	ED Incident Handling Procedures, V 7.1, April 2003	Appendix B- Incident Reporting and Response Guidance
		Ensure that suspicious event activity is closely monitored or expand system logging capabilities as directed by the Incident Handling Coordinator, and provide report updates, if necessary on a daily basis.	ED Incident Handling Procedures, V 7.1, April 2003	ED Incident Handling Procedures, V 7.1, April 2003
<b>Data Integrity</b>		Document data integrity procedures to describe how the system detects and prevents any unauthorized alteration or destruction of data.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Data Integrity
		Establish procedures for routine updates to virus signature files, including automatic and/or manual virus scans.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Virus Detection and Elimination
		Establish written procedures if the system requires near real-time performance analysis.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Performance Measurements
		Identify whether the system's availability level can operate using periodic performance sampling or other less demanding controls.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Performance Measurements
		Review system performance procedures at least annually.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Performance Measurements
		Periodically review the system to identify and, eliminate unnecessary services (e.g. FTP, HTTP,).	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Maintenance and Repair

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
		Periodically review the system for known vulnerabilities and current installation of software patches.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Maintenance and Repair
		Ensure that fraud, waste, and abuse prevention policies are supported.	ED Information Technology Security Policy, October 2001	Fraud, Waste, and Abuse
<b>System Security Plan</b>		Have an approved system security plan written in the format and containing the topics prescribed in NIST Special Publication 800-18.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	System Security Plan
		Submit the security plan, and subsequent updates, to the OCIO or his/her designee for review.	ED Information Technology Security Policy, October 2001	Business or Functional Managers
<b>Personnel Security</b>		Establish job descriptions that accurately document assigned duties and responsibilities.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Position Descriptions
		Classify the sensitivity of each position.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Sensitivity/Risk Levels
		Create formal procedures defining the authority granted to each user or class of users.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Segregation of Duties

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
		On at least an annual basis, validate compliance with personnel security controls for all personnel under their supervision.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Compliance
<b>Use of External Connections</b>		Approve all external network connections in advance.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Use of External Connections
<b>Production Input/Output Controls</b>		Establish procedures and protection controls to safeguard the storage of media.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Production Input/Output Controls
		Decide on requests for authorization to use privately owned software.	ED Information Technology Security Policy, October 2001	Incident Reporting and Response
<b>Maintenance and Repair</b>		Develop procedures to restrict or control the activities of those who perform maintenance and repair activities, both on-site and off-site.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Configuration and Management Documentation
		Specify procedures regarding issues such as the escort of maintenance personnel, sanitization of devices removed from the site, etc.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Configuration and Management Documentation
		Describe procedures used to control remote maintenance services.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Maintenance and Repair
		Implement access controls and other security precautions to prevent potentially malicious code, such as "back doors."	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Maintenance and Repair
		Develop procedures to check and correct any deviations in the audit trail clock and machine clock time.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Audit Trails
<b>Testing</b>		Periodically test security control policies, procedures and techniques, and fix noted deficiencies found during these testing.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Security Control Reviews
		Budget for and conduct an annual routine self-assessment, in NIST 800-26 format.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Security Control Reviews

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
		Implement risk mitigation actions to bring the system risk to an accept level for the Designated Approval Authority.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Security Control Reviews
		At least annually, conduct and document tests of the Continuity of Support Plan /disaster recovery plans.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Plan Maintenance
		Prescribe and document the acceptable time frames for reconstitution of system functions prior to the beginning of COS/ disaster recovery testing to ensure that timely reconstitution is not sacrificed to achieve a "successful" test.	ED Information Technology Security Policy, October 2001	Continuity of Operations Planning
		Inform the DAA of the results of COOS/disaster recovery testing and any resulting readjustments to the plans.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Plan Maintenance
		Oversee penetration testing performed on their system(s).	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Penetration Testing
<b>Passwords</b>		Select and authorize personnel to use password compliance tools.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Passwords
		Record the password compliance authorization and specify the locations, systems and duration covered by the authorization.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Passwords
<b>Logical Access Controls</b>		Establish procedures to restrict and control access to all program libraries, system software, and system hardware.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Logical Access Controls
		Assign a person(s) to review protocols with known vulnerabilities, such as UDP and TFTP, and receive approval for their use prior to implementation from the System Owner and the DAA.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Logical Access Controls

Topic	#	Responsibility	Document	Section
		Assign an employee to create and maintain a current list of authorized users and their access levels.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Access Control List
		Approve the access control list before its implementation.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Access Control List
		Review and decide upon requests to telecommute.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Remote Access
<b>Physical Access Controls</b>		Limit access to controlled areas and sensitive IT resources to only personnel who have a security screening commensurate with the sensitivity of the data accessed and have a valid need for access.	ED Information Technology Security Policy, October 2001	Physical Security
		Establish appropriate procedures to control the access to, and use of, terminal equipment within their respective offices.	ED Information Technology Security Policy, October 2001	Workstation and Desktop Security

Topic	#	Responsibility	Document	Section
<b>Documentation</b>		Maintain the following documentation for all FSA Major Applications and General Support Systems: <ul style="list-style-type: none"> <li>• A current System Security Plan.</li> <li>• C&amp;A documents and authorizing statements, including all required appendices.</li> <li>• A log of service packs, patches upgrades, etc. for the system, and the order of installation.</li> <li>• A network diagram and documentation on placement and configuration of firewalls, intrusion detection sensors or other security software or appliances.</li> <li>• Standard operating procedures.</li> <li>• Software/hardware user manuals.</li> <li>• Vendor-supplied documentation of software and hardware.</li> <li>• Application documentation, requirements, and specifications per the system's current contract.</li> <li>• Software/hardware testing procedures and results.</li> </ul>	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Documentation
<b>Contractors</b>		Work with contracting officers or their representatives to ensure contractor compliance with the Department's security policies.	ED Information Technology Security Policy, October 2001	Personnel Security
		May authorize any qualified Department employee to perform a review of contractor proposals to determine the adequacy and the capability of the prospective awardees to meet the stipulated security requirements.	ED Information Technology Security Policy, October 2001	Personnel Security
<b>SYSTEM SECURITY</b>				

Topic	#	Responsibility	Document	Section
<b>OFFICER</b>				
<b>Solution Life Cycle</b>		Review the business case and ensure it includes the necessary resources for adequately securing the system.	FSA System Security Process Guide, V 3.0, March 2003	Vision Phase
		Complete the GSS/MA Inventory worksheet.	FSA System Security Process Guide, V 3.0, March 2003	Definition Phase
		Distribute, educate on, and maintain signed copies of the following from system users: <ul style="list-style-type: none"> <li>• Rules of Behavior forms</li> <li>• Background clearance forms</li> <li>• System user access forms</li> </ul>	FSA System Security Process Guide, V 3.0, March 2003	Definition Phase
		Obtain and review MOU/ISA/TPAs for inclusion of appropriate security controls.	FSA System Security Process Guide, V 3.0, March 2003	Construction Phase
		The SSO should attend the PRR as a security representative to respond to any concerns presented during the PRR.	FSA System Security Process Guide, V 3.0, March 2003	Deployment Phase
		When the system will no longer be in use, create an archive data retention matrix and destruction plan.	FSA System Security Process Guide, V 3.0, March 2003	Retirement Phase
		Complete all of the phase checklists and submit to the System Manager for signature.	FSA System Security Process Guide, V 3.0, March 2003	Retirement Phase
<b>Continuity of Support (COS)/ Contingency Planning</b>		Coordinates the creation, implements and updates the Continuity of Support Plan.	FSA System Security Process Guide, V 3.0, March 2003	Appendix A
		Complete the COS Plan prior to the authorization process starting.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Contingency Planning
		Distribute the COS Plan to appropriate personnel.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Contingency Planning
	The system manager, SSO, and CSO must review	FSA Information Technology	Contingency	

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
		and approve the Continuity of Support Plan and apprise the System Owner of updated versions.	Security and Privacy Policy, V 2.0, April 2003	Planning
		Participate as a member in contingency program subteams.	ED Information Technology Contingency Planning Procedures, February 2003	Contingency Planning Coordinator
		If there is a contingency event that affects/disrupts the operation with an interconnected system, the SSO must contact/ inform the designated system counterpart.	FSA Memorandum of Understanding, V 1.0, June 2003	Communications
<b>Certification and Accreditation</b>		Participate in the C&A process including being a member of the C&A Team.	ED IT Security SDLC Security Integration Guide, V 3.0, Sept 2002	Phase 1: Planning
		Along with the project team, develop the C&A project plan.	FSA System Security Process Guide, V 3.0, March 2003	Definition Phase
		Obtain a copy of the signed accreditation letter.	FSA System Security Process Guide, V 3.0, March 2003	Deployment Phase
<b>Configuration Management</b>		Review possible changes and recommend approval or disapproval of the change based on the risk to the security of the system.	ED Information Technology Security Policy, October 2001	Configuration Management
<b>Intrusion Detection</b>		Keep abreast of the status of intrusion detection related issues.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Intrusion Detection
<b>Training</b>		Complete personal security training.	FSA System Security Process Guide, V 3.0, March 2003	Definition Phase
		The SSO also is responsible for training requirements, namely rules of behavior and security awareness training. Direct all new users to receive security awareness training.	FSA System Security Process Guide, V 3.0, March 2003	Support Period

Topic	#	Responsibility	Document	Section
<b>Account Access</b>		The SSO should review and authorize system access privileges on a per case basis, provide periodic review of user access privileges and delete user accounts as necessary.	FSA System Security Process Guide, V 3.0, March 2003	Support Phase
		Before granting initial access to an FSA system, verify the following: <ul style="list-style-type: none"> <li>• The user has authorization from the system owner and supervisor to access the system,</li> <li>• The level of access is appropriate for the user's business purpose,</li> <li>• The access will not compromise segregation of duties,</li> <li>• The user received a copy of the Rules of Behavior for the system and has signed a statement indicating that he/she understands and agrees to the Rules, and</li> <li>• Completion (for high-risk positions) or initiation (for low-medium risk positions of proper background screening).</li> </ul>	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Identification and Authentication
		Use a documented process for requesting, establishing, issuing, and closing all user accounts.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Establishing and Terminating Accounts
		Identify any system privileges or features, which would allow a user to override system or application controls, and associate these privileges with the categories of staff that would use them.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Establishing and Terminating Accounts
		Maintain a system authorization process and record of privileges.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Establishing and Terminating Accounts
		Review authorization for privileged access rights at least quarterly to see if privileged access is still required, and to make sure users have not been	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Establishing and Terminating Accounts

Topic	#	Responsibility	Document	Section
		erroneously assigned unauthorized privileges.		
		Within documentation, include actions taken when the limit is exceeded for logon attempts.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Identification and Authentication
<b>Incident Response</b>		<p>Incidents are classified as either Category A or Category B. For Category A incidents, the SSO must log and track the incidents by system and prepare a monthly report to the OCIO Incident Handling Coordinator, submitted no later than the 4<sup>th</sup> day of the month following the month in which the event is discovered.</p> <p>For Category B incidents, the SSO must log and track the incidents by system and prepare a report for the OCIO Incident Handling Coordinator, submitted no later than the 4<sup>th</sup> day of the week following the week in which the event is discovered.</p>	ED Incident Handling Procedures, V 7.1, April 2003	Appendix C- Types of Incidents and Suspicious Activities
		Issue a “confirmation of receipt” to the party reporting an incident.	ED Incident Handling Procedures, V 7.1, April 2003	Reporting an Incident
		Report security incidents to the CSO within one hour of receiving the Suspicious Event Report (SER). Send the CSO the SER.	<p>FSA Information Technology Security and Privacy Policy, V 2.0, April 2003</p> <p>ED Incident Handling Procedures, V 7.1, April 2003</p>	<p>Incident Identification</p> <p>Appendix B- Incident Reporting and Response Guidance</p>
		Perform corrective actions as directed in response to a reported incident.	ED Incident Handling Procedures, V 7.1, April 2003	System Security Officer
		Collect and secure audit trails and other tracking mechanisms for analysis and use as potential evidence.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Post Incident Activities
		Generally recommended protective measures to consider regarding potential IT evidence.	ED Incident Handling Procedures, V 7.1, April 2003	System Security Officer

Topic	#	Responsibility	Document	Section
		Review incident handling procedures and control techniques with the SM after each incident and, when necessary, modify the procedures to prevent recurrence and improve response techniques/methods.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Post Incident Activities
		Maintain contact with other security offices within the Department that focus on mission essential protection that are capable of providing indications and warnings for the Department's critical assets.	ED Information Technology Security Policy, October 2001	System Security Officer
		Review and implement incident handling procedures and maintain an adequate reporting capability.	ED Information Technology Security Program Management Plan, April 2003	Risk Management Sub-program Element – Incident Response

Topic	#	Responsibility	Document	Section
		If, during system log reviews, a suspicious event is discovered, the system administrator, SSO or system manager will categorize the event according to the Department's Schedule B – Incident Reporting & Response Guidance – Suspicious Event Matrix.	ED Incident Handling Procedures, V 7.1, April 2003	Appendix B- Incident Reporting and Response Guidance
		Category “A” type suspicious events (those which are effectively countered by security controls in place) will be logged and tracked by the system SSO.	ED Incident Handling Procedures, V 7.1, April 2003	Appendix B- Incident Reporting and Response Guidance
		If an incident occurs that will affect an interconnected system, the SSO must contact/ inform the security counterpart of the incident.	FSA Memorandum of Understanding, V 1.0, June 2003	Communications
		If an incident occurs that will affect an interconnected system, the SSO must provide a formal report regarding the incident to the counterpart system owner within 5 business days of the detection.	FSA Memorandum of Understanding, V 1.0, June 2003	Communications
		<p>Expected to know the following:</p> <ul style="list-style-type: none"> <li>• Department security policies for IT systems</li> <li>• Common security threats</li> <li>• Capability of recognizing system anomalies and assessing the impact of threats posed by those anomalies</li> <li>• Methods used to recover from security breaches</li> <li>• Methods used to prevent security breaches</li> <li>• General technical knowledge of system to coordinate responses to a security breach</li> <li>• Generally recommended protective measures regarding potential evidence</li> <li>• Evidence preservation techniques</li> </ul>	ED Incident Handling Procedures, V 7.1, April 2003	System Security Officer
<b>Data Integrity</b>		Authorize the transfer of sensitive information from a central computer or server to any device having the	ED Information Technology Security Policy, October 2001	Workstation and Desktop Security

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
		capability to record information on magnetic or other media.		
<b>Security Plan</b>		Review and update the security plan at least annually to reflect current conditions and risks.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	System Security Plan
<b>Job Descriptions</b>		Use the SM approved job descriptions when designating the sensitivity levels of the positions.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Position Descriptions
<b>Disaster Recovery</b>		Coordinates the creation, implements and updates the Disaster Recovery Plan.	FSA System Security Process Guide, V 3.0, March 2003	Appendix A
		If there is a disaster that affects/disrupts the operation with an interconnected system, the SSO must contact/inform the designated system counterpart.	FSA Memorandum of Understanding, V 1.0, June 2003	Communications
<b>Penetration Testing</b>		Record/review results of penetration testing and report on the ensuing corrective actions.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Penetration Testing
<b>Identification and Authentication</b>		When an FSA system allows bypassing of user authentication requirements, (for example, single-sign-on technologies), document the governing procedures, and compensating controls and whether emergency or temporary access is authorized.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Identification and Authentication
<b>Passwords</b>		Document password procedures for the system.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Passwords
<b>Remote Access</b>		Along with the SSO, review and decide upon requests to telecommute.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Remote Access
<b>Audit Trails</b>		Approve authorization to view audit logs.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Audit Trails
		The SSO will be able to selectively audit the actions of any user(s) based on individual identity.	ED Information Technology Security Policy, October 2001	Audit

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
		Audit records shall be protected so that access is limited to the CSO, the SSO, and other authorized individuals.	ED Information Technology Security Policy, October 2001	Audit
<b>Keystroke Monitoring</b>		If the system uses keystroke monitoring, document the procedures and provide a means of user notification.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Audit Trails
<b>Risk Assessment</b>		Oversee and review risk assessments for the assigned system.	ED Information Technology Security Policy, October 2001	System Security Officer
<b>Websites</b>		If the system collects information from the public from a website, during the Definition Phase of the FSA Solution Lifecycle, the SSO must complete the FSA Privacy Impact Assessment Questionnaire and file the form in the system's Security.	FSA Privacy Impact Assessment and Privacy Notice for Websites	Introduction
<b>Contracts</b>		Along with the CSO, ensure that all appropriate security requirements are included in all statements of work and that appropriate risk levels are assigned to each position	ED Information Technology Security Policy, October 2001	Contracts and Solicitations
<b>Documentation</b>		The SSO should establish a paper and an electronic based filing system to adequately maintain, update, protect and distribute system documentation. The SSO should manage version control of all security documentation and track the distribution of security artifact copies.	FSA System Security Process Guide, V 3.0, March 2003	Vision Phase
		Document procedures from the SM regarding as the escort of maintenance personnel, sanitization of devices removed from the site in a Configuration Management Plan and/or in the system's security plan.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Configuration and Management Documentation
		Summary of Documents the SSO must review and maintain:		

Topic	#	Responsibility	Document	Section
		<ul style="list-style-type: none"> <li>• GSS/MA Inventory worksheet</li> <li>• C&amp;A Project Plan</li> <li>• MOU/TPA/ISAs</li> <li>• System’s correction action plan (developed based upon the results of the risk assessment.)</li> <li>• A copy of the signed accreditation letter</li> </ul> Signed copies of the following: <ul style="list-style-type: none"> <li>• Rules of Behavior forms</li> <li>• Background clearance forms</li> <li>• System user access forms</li> <li>• Archive data retention matrix and destruction plan</li> <li>• Disaster Recovery Plan</li> <li>• Continuity of Support Plan</li> <li>• System Security Plan</li> </ul>		
		Know the locations of all required documentation.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Documentation
<b>SYSTEM ADMINISTRATOR (SA)</b>				

Topic	#	Responsibility	Document	Section
		Ensure that the SSO/NSO is aware of all matters that concern the security of the systems for which they are responsible.	ED Incident Handling Procedures, V 7.1, April 2003	System Administrator/Network Security Officer
		Notify SSO of suspicious events weekly and advise them if the event should be classified as a Category A or B suspicious event (See Appendix C.)	ED Incident Handling Procedures, V 7.1, April 2003	Appendix C- Types of Incidents and Suspicious Activities
		If the SA identifies an incident, fill out the Department's Suspicious Event Reporting (SER) form.	ED Incident Handling Procedures, V 7.1, April 2003	
		Notify the SSO of an incident immediately and give them the completed SER form.	ED Incident Handling Procedures, V 7.1, April 2003	Appendix B- Incident Reporting and Response Guidelines
		The SSO or system administrator must notify their Principal Office CSO by telephone, email or fax within <b>one (1) hour</b> of receiving the initial Suspicious Event Report (SER). If the PO CSO is not available by telephone, email or fax, the reporting party must notify the OCIO Incident Handling Coordinator using the same process and receipt confirmation. <i>If the OCIO Incident Handling Coordinator has not confirmed receipt within one (1) hour of notification, the reporting party must notify the Deputy CIO using the same process and receipt confirmation.</i>	ED Incident Handling Procedures, V 7.1, April 2003	Appendix B- Incident Reporting and Response Guidelines
		Ensure you receive a confirmation of receipt when reporting an incident and note the time the receipt was received.	ED Incident Handling Procedures, V 7.1, April 2003	Appendix B- Incident Reporting and Response Guidelines
<b>Incident Response</b>		If, during system log reviews, a suspicious event is discovered, the system administrator, SSO or system manager will categorize the event according to the Department's Schedule B – Incident Reporting & Response Guidance – Suspicious Event Matrix.	ED Incident Handling Procedures, V 7.1, April 2003	Appendix B- Incident Reporting and Response Guidance

Topic	#	Responsibility	Document	Section
		If there is an event involving a Department's computer, be prepared to offer assistance, such as completing the Department's Incident Notification Checklist and the Chain of Custody form.	ED Incident Handling Procedures, V 7.1, April 2003	
		Conduct regular security log reviews and periodic log audits of the network	ED Incident Handling Procedures, V 7.1, April 2003	System Administrator/Network Security Officer
		Identify and report to the SSO/NSO any inconsistencies or irregularities in system log entries or usage that may signify a security incident.	ED Incident Handling Procedures, V 7.1, April 2003	System Administrator/Network Security Officer
		<p>Expected to know the following:</p> <ul style="list-style-type: none"> <li>• Department security policies for IT systems</li> <li>• Common security threats</li> <li>• Capability of recognizing system anomalies and assessing the impact of threats posed by those anomalies</li> <li>• How to quickly assess the overall aspects of an incident and identify IT equipment, which should be suspected of being associated with the incident.</li> <li>• Methods used to recover from security breaches</li> <li>• Methods used to prevent security breaches</li> <li>• General technical knowledge of the system to coordinate responses to a security breach</li> <li>• Generally recommended protective measures regarding potential IT evidence.</li> <li>• Preservation of evidence techniques</li> </ul>	ED Incident Handling Procedures, V 7.1, April 2003	System Administrator/Network Security Officer

Topic	#	Responsibility	Document	Section
<b>USERS</b>				
<b>Training</b>		Attend annual security awareness training.	FSA System Security Process Guide, V 3.0, March 2003	Support Period
<b>Account Access</b>		When first obtaining system access, sign and return the following documents to the SSO: <ul style="list-style-type: none"> <li>• Rules of Behavior forms</li> <li>• Background clearance forms</li> <li>• System user access forms</li> <li>• Nondisclosure and/or confidentiality agreement (if accessing sensitive information)</li> </ul>	FSA System Security Process Guide, V 3.0, March 2003	Definition Phase
		Maintain the confidentiality, integrity and availability of FSA information systems.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Security and Privacy Awareness and Training
		User activity will be audited and monitored and access restricted to authorized functions only, in accordance with the <i>Worldwide Web Server Policy and Procedures</i> .	ED Information Technology Security Policy, October 2001	Web Site Operations
<b>Incident Response</b>		Non-security personnel must never attempt to prove suspected weaknesses on their own, as FSA must treat this act as an actual attack that may result in heavy penalties.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Incident Identification
		Notify FSA System Managers, SSO, and/or system administrators as soon as possible regarding any observed or suspected security weaknesses in, or threats to systems or services or security problems, suspicious events or incidents.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003 ED Incident Handling Procedures, V 7.1, April 2003	Incident Identification Employees and System Users
		Report software malfunctions to FSA System Managers, SSO, and/or system administrators as soon as possible.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Incident Identification
		Report viruses, password security, and Rules of	ED Incident Handling Procedures, V	Employees and

Topic	#	Responsibility	Document	Section
		Behavior violations to the SSO or other appropriate security officer.	7.1, April 2003	System Users
		If an incident is declared, follow the direction of the CSO and the Department's OCIO Incident Handling Coordinator throughout the duration of the security event investigation.	ED Incident Handling Procedures, V 7.1, April 2003	Appendix B- Incident Reporting and Response Guidance
		<p>Employees and System Users are expected to know the following:</p> <ul style="list-style-type: none"> <li>• Department information security policies and procedures</li> <li>• How and to whom to report a security incident violation – (See Appendix A -- OCIO Incident Handling Guidelines Memo)</li> <li>• How to recognize workstation anomalies</li> <li>• Methods used to prevent security breaches at the user's workstation.</li> </ul>	ED Incident Handling Procedures, V 7.1, April 2003	Employees and System Users
<b>Physical Access</b>		Securely store unused keys, keycards or other entry devices used to enter sensitive areas and return these devices when no longer needed.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Physical Access Controls
		Obtain and display their FSA identification badges at all times, regardless of the area's sensitivity.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Physical Access Controls
		Restrict access to sensitive areas to authorized personnel only and grant access in a way that creates an audit trail.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Physical Access Controls
		Report all suspicious activity and/or security violations to management officials.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Physical Access Controls
		Locate computer monitors displaying sensitive data in areas that prevent viewing by unauthorized personnel.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Physical Access Controls

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
		Restrict and monitor physical access to data and telecommunication transmission lines and their housing facilities.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Physical Access Controls
		Encrypt data files that contain information designated as "sensitive" on portable/mobile devices.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Physical Access Controls
		Log out when leaving terminals, workstations, and networked personal computers unattended.	ED Information Technology Risk Assessment Guide, V 6.2, July 31, 2002	Technical Controls I&A
<b>Portable Computers</b>		Individuals in possession of portable computers or storage media containing sensitive FSA information must not leave such equipment unattended at any time unless the information has been properly safeguarded. Such individuals take full responsibility and accountability for the equipment and the data it contains.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Use of External Connections
<b>Data Controls</b>		Ensure that unauthorized individuals cannot read, copy, alter or remove any printed or electronic information for their own use or the use of another.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Production Input/Output Controls
		Only authorized users may pick up, receive, or deliver input and output information and media.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Production Input/Output Controls
		Externally label all media for sensitivity and include any special handling instructions on the label for mailing purposes.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Production Input/Output Controls
		Shred or destroy sensitive hardcopy media when no longer needed or when damaged/spoiled.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Production Input/Output Controls
		Sanitize FSA electronic media for reuse, storage or destruction when no longer needed or if it becomes damaged/spoiled.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Production Input/Output Controls

Topic	#	Responsibility	Document	Section
		Scan untrusted removable media for viruses.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Virus Detection and Elimination
		Do not post Department records (e.g., software, internal memos, internal policies, Department information and data) on any publicly accessible Internet site unless the posting is approved in writing by an appropriate senior level Department official.	ED Information Technology Security Policy, October 2001	Internet and Intranet Security
		Ensure that fraud, waste, and abuse prevention policies are supported; including: <ul style="list-style-type: none"> <li>• Not using government computers for personal business</li> <li>• Not tampering with government information</li> <li>• Unauthorized usage of Department networks to connect to other networks.</li> </ul>	ED Information Technology Security Policy, October 2001	Fraud, Waste, and Abuse
<b>Intrusion Detection</b>		Inform the System Owner whenever intrusion detection tools are implemented or modified.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Intrusion Detection
		Do not scan or probe security mechanisms at either Department or other Internet sites unless they have first obtained permission from the CIO or his/her designee for the purpose of penetration testing.	ED Information Technology Security Policy, October 2001	Internet and Intranet Security
		Do not establish Internet or other external network connections that could allow unauthorized non-Department users to by-pass security features and gain access to Department systems and information.	ED Information Technology Security Policy, October 2001	Internet and Intranet Security
<b>Software</b>		Software installation and use follows the principle that whatever is not expressly allowed is denied.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Unapproved Software
		Installation of personal software on Department assets is prohibited unless approved in writing from	FSA Information Technology Security and Privacy Policy, V 2.0,	Unapproved Software

<b>Topic</b>	<b>#</b>	<b>Responsibility</b>	<b>Document</b>	<b>Section</b>
		the Department CIO.	April 2003	
		If personally owned software is used for FSA business, document each instance including provisions to protect software copyrights and inform their supervisor in writing.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Unapproved Software
		Use of software in a manner that is not consistent with the vendor's license is prohibited.	ED Information Technology Security Policy, October 2001	Internet and Intranet Security
<b>Passwords</b>		If users are given a temporary password, they must change it as soon as they login.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Passwords
		Do not write down or reveal passwords to anyone.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Passwords
		Change your password at least every ninety days or earlier if needed.	FSA Information Technology Security and Privacy Policy, V 2.0, April 2003	Passwords