

Organization	Document	Date	Location- either at website or in the C&A folder with the file name listed	Description
Definition				Certification and accreditation (C&A) is the periodic, independent verification and validation that existing risk management has been effectively implemented. C&A is mandated by OMB Circular A-130 and must be completed for all GSSs/MAs at least every 3 years.
Federal Policy				This is the full version of the E-Gov Act. Of particular interest is Title III (FISMA), which addresses, among other things, security testing and evaluation.
	E-Government Act (Public Law 107-347)	Dec-02	http://www.aiprp.gov.qc.ca/publications/pdf/getdoc%5B1%5D.pdf	
NIST	NIST 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems	6/1/03	http://csrc.nist.gov/publications/drafts/sp800-37-Draftver2.pdf	This NIST document provides guidelines for certifying and accrediting federal information systems. Topics include roles and responsibilities, C&A boundaries, and the process for C&A.
ED Policy	Department of Education Information Technology Security Certification and Accreditation Program Overview	6/1/03	http://connected/doc/img/ED%20CA%20Program%20Overview.doc	The purpose of this Certification & Accreditation (C&A) Program Overview is to provide management personnel with a "road map" that clearly describes how the Department will implement the C&A program. The plan outlines specific roles and responsibilities.

	<p>Department of Education Information Technology Security</p> <p>Information Technology Security Handbook for Certification and Accreditation Procedures</p>	<p>2/1/03 http://connected/doc/img/ED%20CA%20Procedures%20v6.22.doc</p>	<p>Individuals responsible for, or involved in, the C&A process can use these procedures as a resource to certify and accredit the Department's GSSs (general support systems) and MAs (major applications). In addition to defining the C&A process, this document also address several fundamental questions related to the C&A process.</p>
	<p>Department of Education Information Technology Security Program</p> <p>Information Technology Security Test & Evaluation Guide</p>	<p>6/1/03 http://connected/doc/img/ED_STE%20Guide%20v5.doc</p>	<p>This Security Test and Evaluation (ST&E) Guide provides an overview of the content and role of an ST&E Test Plan as it relates to Certification and Accreditation (C&A) of all of the Department's GSS and MAs. It establishes the Department's parameters and and minimum standards for an ST&E.</p>
<p>FSA Policy Tools</p>	<p>C&A System Inventory File</p>	<p>3/3/03 Folder- C&A_System_Inventory_File</p>	<p>This tool can be used in the information-gathering stage of C&A to organize what hardware and software is located at each facility that a system uses.</p>
	<p>C&A System Boundaries and Interconnections</p>	<p>3/3/03 Folder- C&A_System_Boundaries_and_Interconnections</p>	<p>This tool can be used in the information-gathering stage of C&A to map out all the system interconnections that a system has. The second part is a section for describing the data flow associated with each system interconnection.</p>

Training

FSA C&A Training

4/1/03 Folder

FSA_C&A_training

For More Info

NIST Certification
and Accreditation
homepage

[http://csrc.nist.gov/sec-
cert/](http://csrc.nist.gov/sec-cert/)

Contacts

[Jeff Keyes \(hyperlink
to email
jeff.keyes@ed.gov\)](#)

Organization	Document	Date	Location- either at website or in the configuration management folder with the file name listed	Description
Definition				<p>Required Plan: Configuration Management Plan (Tiers 1, 2, 3, 4)</p> <p>Configuration Management is defined as the systematic identification, documentation, and control of system elements by recording and reporting change processing and implementation status. These activities assist in verifying compliance with specified system requirements as well as maintaining the technical integrity of a system throughout its life cycle. The successful implementation of CM activities results in an established and documented system baseline, effective management and tracking of changes made to a GSS/MA and related documentation (version control), and effective risk management.</p>
Federal Regulations				
NIST				
ED	Department of Education Handbook for Information Technology Security Configuration Management Planning Procedures	5/13/03	http://connected/doc_img/Handbook%20for%20Config%20Mgmt%20Procedures%20Final.doc	This handbook provides the Department's approach to developing a configuration management plan (CMP). The handbook provides guidance to the individuals responsible for, or involved in the configuration management (CM).

FSA				
Tools	Configuration Management Plan Checklist	Jan 6 2003	folder-configuration_mngt_plan_checklist_jan03	This checklist is a way to verify that a system's configuration management plan meets all of the requirements of the Department.
Training	ED Configuration Management Training	Feb-03	folder-ED_Configuration_Mgmt_Training_feb03	
For More Information	CM Today		http://www.cmtoday.com/	
Contacts	Derek Foxley (hyperlink to derek.foxley@ed.gov)			

Organization	Document	Date	Location- either at website or in the data classification folder with the file name listed	Description
Definition				Information within the Department is classified differently, according to
Federal Regulation				
NIST				
ED	Protecting Sensitive But Unclassified Information Memo	May-03 folder-	OCIO_Protecting_Sensitive_But_Unclassified_Information_memo_may2003	This memo reminds the Department of the importance of handling SBU information and references Chapter 11 in the Information Security handbook for additional information.
	Description of FOIA	May-03 folder-	OCIO_SBU_AttachmentA_FOIA	This document is a high level overview of FOIA and how it relates to the Privacy Act.
	Principal Officer Coordinators Office	May-03 folder-	OCIO_SBU_AttachmentB_Principal_Office_Coordinator_list	This document is a listing of the different Principal Office Coordinators.
FSA				
Tools				
Training				
For More Information	Data Classification white paper		http://www.emc.com/global_services/isc/pdf/c1059_data_classification_the_cornerstone_for_successful_ilm_white_paper_1dv.pdf	
Contacts	Brian Fuller (hvnerlink email to			

Organization	Document	Date	Location- either at website or in the privacy folder with the file name listed	Description
Definition				Required Plans: Privacy Impact Assessment, depending on the system (Tiers 1, 2, 3, 4)
Federal	Privacy Act		http://www.usdoj.gov/04foia/privstat.htm	This is a link to the full text of the Privacy Act.
	E-Government Act (Public Law 107-347)	Dec-02	http://www.aiprp.gouv.qc.ca/publications/pdf/getdoc%5B1%5D.pdf	This is the full version of the E-Gov Act. Of particular interest is Section 208, which deals with privacy impact assessments.
NIST				
ED				
FSA Tools	Privacy Impact Assessment Template	Jul-03	privacy folder- privacy_impact_assessment_template_ July2003	This is a template for a privacy impact assessment along with an explanation of when a privacy impact assessment needs to be performed.
Training	FSA Privacy Impact Assessment Training	Aug-03	folder- privacy_impact_assessment_training_2003	
For More Information	More Information On E-Government Act		http://www.egov.vic.gov.au/International/TheAmericas/UnitedStates/E-government-Act-2002/e-government-act-2002.htm#implementationguidance	
	High Level Overview of E-Government Act OMB Guidance for Implementing the Privacy Provisions of the E-Gov Act	Jun-03	folder- e-gov_act_overview http://www.whitehouse.gov/omb/memoranda/m03-22.html	This document is a high level overview of the E-Government Act.
Contacts	Jill Mossman (hyperlink to email to jill.mossman@ed.gov)			

Organization	Document	Date	Location- either at website or in the system security plan folder with the file name listed	Description
Definition				<p>Required Plan: System security plan (Tiers 1, 2, 3, 4)</p> <p>Security controls that are documented in the security plan are policies, procedures, and practices designed to provide a level of assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. The plan consists of three main areas (management, operational, and technical) of IT security controls identified by NIST, when properly implemented, can reduce the likelihood that a system vulnerability is exploited and limit the potential damage to IT and organizational resources.</p>
Federal	NIST 800-18 Guide for Developing Security Plans for Information Technology Systems	Dec-98	http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.doc	This publication details the specific management, technical and operational controls that should be documented in a system security plan.

ED Department of Education Information Technology Security Program Information Technology Security Controls Reference Guide Jun-03 http://connected/doc_img/ED%20Security%20Controls%20Reference%20Guide%20v5.doc This Guide is intended to provide an overview and reference of management, operational, and technical security controls.

FSA
Tools

Training ED System Security Plan Training Jan-02 folder-ed_security_plan_training

For More Information

Contacts Chuck Tobler (email hyperlink to ctobler@bearingpoint.net)

Organization	Document	Date	Location- either at website or in the system interconnections folder with the file name listed	Description
Definitions				<p>Required Plans: If any Tier system exchanges information with another <u>government system</u>, they need to fill out the appropriate system interconnection document.</p> <p>Systems rarely operate in a vacuum. They frequently depend upon other systems or vice versa for information necessary to their mission or processing activities. System interconnection documents are a way to formally describe the responsibilities of each system in exchanging information.</p>
Federal NIST	NIST 800-47 Security Guide for Interconnecting Information Technology Systems	Aug-02	http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf	The Security Guide for Interconnecting Information Technology Systems provides guidance for planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations.
ED FSA Tools	FSA System Interconnection Template Explanations	Aug-03	folder- fsa_system_interconnection_template_explanations	This document is a high level overview describing the different system interconnection templates and when it is appropriate to use each one.

FSA MOU
Template

Aug-03 folder-
fsa_mou_template_ aug
2003

When creating a system interconnection with a government system located outside of Department of Education, use the FSA Interconnection Security Agreement and the FSA Memorandum of Understanding.

FSA Trading
Partner Agreement
Template

Aug-03 folder-
fsa_tpa_template_ aug
2003

For system interconnections between systems located within the Department of Education, use the FSA Trading Partner Agreement.

FSA
Interconnection
Security Agreement
Template

Aug-03 folder-
fsa_isa_template_
Aug2003

When creating a system interconnection with a government system located outside of Department of Education, use the FSA Interconnection Security Agreement and the FSA Memorandum of Understanding.

Training

For More
Information

Contacts

Jill Mossman
([hyperlink to email to jill.mossman@ed.gov](mailto:jill.mossman@ed.gov))

Definition	Document	Date	Location	Description
				<p>Required Evaluation: Risk Assessment (Tiers 1, 2, 3, 4) Corrective Action Plan (Tiers 1, 2, 3, 4)</p> <p>Risk is a measure of the degree to which information resources are exposed based on the exploitation of a vulnerability by a potential threat. Risk is composed of two elements: 1) the <u>impact</u> that an exploited vulnerability would have on the organization's mission or operations; and 2) the <u>likelihood</u> that such an exploitation would occur. A risk assessment is the process of analyzing and then interpreting risk associated with potential threats and vulnerabilities. The risk assessment acts as a means to help evaluate the effectiveness of various security controls in place for each GSS or MA. A corrective action plan takes the results of the risk assessment and maps them to corrective actions in order to mitigate the vulnerabilities found in the risk assessment.</p>
Federal NIST	NIST 800-26 Security Self-Assessment Guide for Information Technology Systems	1-Nov	http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf	This document from the National Institute of Standards and Technology (NIST) is a Special Publication (SP) document. This document provides a method for agency officials to determine the current status of their information technology security programs and where necessary, establish a target for improvement. This self-assessment guide utilizes an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems can be tested and measured.

ED	Department of Education, Handbook for Information Technology Security Risk Assessment Procedures	5/12/2003 http://connected/doc_img/Risk%20Assessment%20Procedures%20Final.doc	These Department issued procedures may be used by a system to: 1) perform risk assessments during all stages of the system's life cycle; 2) provide guidance to contractors responsible for developing a system in preparation for an independent risk assessment; and/or 3) understand the risk assessment reports performed by the independent risk assessor.
FSA Tools			
Training	ED Risk Assessment Training	Nov-01 folder-ed_risk_assessment_training	
For More Information	GAO Information Security Risk Assessment	http://www.gao.gov/special.pubs/ai00033.pdf	
Contacts	Brian Fuller (hyperlink email to brian.fuller@ed.gov)		

Organization Definition	Document	Date	Location	Description Required Plans: Continuity of Support (Tiers 1, 2, 3, and 4) Disaster Recovery (Tiers 3 and 4)
Federal NIST	NIST 800-34 Contingency Planning Guide for Information Technology Systems	Jun-02	http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf	<p>Also referred to in FSA as “contingency planning” or “continuity of operations, or COOP,” continuity of support refers to interim measures to recover IT services following an emergency or system disruption. (Note: “COOP” is the term used by Ed. to describe activities otherwise known as Disaster Recovery, Business Continuity, Business Resumption, or Contingency planning.)</p> <p>Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods. The Continuity of Support Plans and disaster recovery plans must have detailed procedures for restoring operation of the system, including the personnel responsible and the timeline within which the FSA system must be returned to normal business operations. FSA continuity of support includes contingency planning as well as disaster recovery. Systems are divided into different Tier levels based upon their evaluated s</p> <p>NIST Special Publication 800-34, Contingency Planning Guide for Information Technology (IT) Systems provides instructions, recommendations, and considerations for government IT contingency planning.</p>

ED

Department of Education,
Handbook for Information
Technology Security Contingency
Planning Procedures

6/12/2003

http://connected/doc_img/Handbook%20for%20Contingency%20Planning%20Procedure%20Final.doc

The purpose of this document is to provide Department system owners with guidance on developing IT contingency plans for their general support systems (GSS) and major applications (MA). This procedures document describes requirements for contingency planning and provides information on preventative controls, recovery methods, and the appropriate format for a contingency plan.

FSA
Tools

FSA IT Contingency Planning
Checklist

Jan-03

contingency planning
folder-
fsa_contingency_plan_c

hecklist_Jan2003

This document is intended to assist SSOs and contractors assess existing IT contingency plans and determine compliance with the Department's IT Contingency Planning Guide.

Training

FSA Contingency Planning
Training

Sep-02

contingency planning
folder-
fsa_contingency_plannin

g_training

For Additional
Information

Contacts

Jeff Keyes (hyperlink to email
jeff.keyes@ed.gov)

Organization Definition	Document	Date	Location	Description
Federal NIST ED	Department of Education, Information Technology Security Cost Estimation Guide	Nov-02	http://connected/doc_img/ sec_cost_est_guide.doc	The Information Technology Security Cost Estimation Guide is designed to help Department of Education (ED) personnel with budgeting responsibilities for IT security to estimate the level of effort and cost associated with implementing security controls. Cost estimates discussed in this guide are broken down by specific security controls, which are based on the management, operational, and technical controls in NIST 800-26.
FSA Tools	ED Cost Estimation Guide Training	2002	cost guide folder- ed_cost_estimation_traini ng <a href="http://www.cio.com/archiv
e/021502/security.html">http://www.cio.com/archiv e/021502/security.html	
For Additional Info	Return on Investment article			
Contacts	Bob Clayton (email hyperlink to robert.clayton@ed.gov)			

Organization Definition	Document	Date	Location	Description Required Plan: System Inventory Worksheet (Tiers 1, 2, 3, 4)
Federal NIST ED	Department of Education, Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures	5/21/2003	http://connect.ed.gov/po/om/executive/print/acs_hb_ocio_9.doc	This document explains the Department's GSS and MA inventory process and how to fill out the inventory worksheet.
FSA Tools				
Training				
For Additional Information				
Contacts	Jeff Keyes (hyperlink to email jeff.keyes@ed.gov)			

Organization Definition	Document	Date	Location	Description
Federal NIST ED	Departmental Directive, Information Security Incident Handling Procedures	6/26/2003	http://connected1.ed.gov/po/om/executive/print/acs_ocio_3_107.doc	This document provides incident-response guidance and procedures to ensure appropriate and expeditious handling of information security incidents that may adversely affect the Department of Education's (Department) normal business operations. These procedures define the incident-handling process, roles and responsibilities and explain how personnel should coordinate and communicate to achieve an effective and timely response to a security incident.
FSA	Derek has to update FSA's and will send to me.			
Tools	Suspicious Event Reporting Form	Aug-03	http://connected/doc_img/Suspicious%20Event%20Report%20Form.doc	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.
Training	Department Incident Handling Training	Jun-03	folder	Training offered by the Department on incident response activities, including a high level overview of how incident response fits into the overall security architecture.
	EDS Incident Response Procedures	Jun-03	folder	This training goes into greater detail about the specific activities to be undertaken to meet the requirements for incident response.
	FSA Incident Response Training	19-Jun-03	folder	This training introduces incident response activities to FSA and explains how they will be implemented.

For Additional
Information

CERT

The Computer Emergency Response Team (CERT) Coordination Center helps coordinate the efforts of teams when responding to large-scale incidents, provide training to incident response professionals, and research the causes of security vulnerabilities, prevention of vulnerabilities, system security improvement, and survivability of large-scale networks.

<http://www.cert.org>

CIAC

The Computer Incident Advisory Capability (CIAC) provides on-call technical assistance and information to Department of Energy (DOE) sites faced with computer security incidents. CIAC also provides: awareness, training, and education; trend, threat, vulnerability data collection and analysis; hoax information and technology watch.

<http://www.ciac.org/ciac/>

FEDCIRC

<http://www.fedcirc.gov>

The Federal Computer Incident Response Capability (FedCIRC) is the central coordination and analysis facility dealing with computer security related issues affecting the civilian agencies and departments of the Federal Government.

Contacts

Derek Foxley
(hyperlink to
derek.foxley@ed.gov)

Organization	Document	Date	Location	Description
Definition				The need to provide protection for federal information systems has been present since computers were first used. Congress has passed several laws relevant to information system security, to meet these policies and legal requirements, federal organizations must consider information system security in all phases of information system management, including the acquisition phase. Including information system security early in the acquisition process for an information system will usually result in less expensive and more effective security than adding security to an operational system. This section presents a framework for incorporating security into all phases of the information system development life cycle (SDLC) process, from initiation to disposal.
Federal NIST	NIST 800-64 Security Considerations in the Information System Development Life Cycle	Oct-03	http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf	The high-level view in Special Publication 800-64, "Security Considerations in the Information System Development Life Cycle," addresses many key concerns from OMB. For years, officials have pushed agencies to consider security from the very beginning of the development of any system or program in order to head off potential incidents and save money later. Including security in the business case for any new system is now a key evaluation factor for determining whether OMB will grant agency budget requests.
ED	Retirement Checklist	Oct-03	solution life cycle folder-retirement_checklist	Systems can use this form when they retire the system to ensure the proper security measures are undertaken.
FSA	Solution Life Cycle Plan	Apr-03	solution life cycle folder-slc_project_plan	This is a project plan to be used in conjunction with the System Security Process Guide that lays out the step-by-step actions that need to be taken to ensure security is properly included in a system's life cycle.
	System Security Process Guide	May-03	folder-system_security_process_guide_may2003	This document describes the different security activities that need to be taken in each phase of a system's life cycle.
Tools Training For More Info Contacts	Jill Mossman (hyperlink to email to jill.mossman@ed.gov)			

Organization Definition	Document	Date	Location	Description
				People are the cornerstone of information security; they design it, implement it, and maintain it. This section has all the information needed personnel security related issues.
ED	Department Directive on Contractor Access	Jun-03	http://connected1.ed.gov/po/om/executive/print/acs_om_5_101_supplement.doc	This Handbook is for use by Principal Office Executive Offices and all other personnel who are responsible for ensuring that contractor employees are appropriately screened. The Handbook furnishes guidance as well as specific requirements for Principal Offices when implementing the Department of Education's policy for "Contractor Employee Personnel Security Screenings."
FSA- System Access	CPS Access Form	Oct-03	folder	
	ezAudit Access Form	Oct-03	folder	
	FMS Access Form	Oct-03	folder	
	FP Data Mart Access Form	Oct-03	folder	
	IFAP Access Form	Oct-03	folder	
	PEPS Access Form for Department employees	Oct-03	folder	
	PEPS Access Form for non-Department employees	Oct-03	folder	
	VDC Access Form	Oct-03	folder	
	eCB Access Form	Oct-03	folder	
	EDNet Access Form	Oct-03	Personnel folder- ednet_access_form	
	DLSS Access Form	Oct-03	personnel folder- system access- dlss_access_form	

Badge	Id Badge Application	Oct-03 http://fsanet/forms/administration/ed_id_card.html	A copy of a blank Department of Education Badge application.
Property pass	Property Pass form	Oct-03 http://fsanet/forms/administration/prop_pass_form.doc	This form is to be used if an employee or contractor will be taking equipment in and out of the building. For example, a contractor might have a company issued laptop that they will be taking in and out of the building.
Background	Guide to Background Clearance paperwork	Oct-03 Personnel folder- clearance stuff folder- guide_to_clearance_paperwork	This is a guide to determining the job risk level of an employee or a contractor and the paperwork associated with each level.
	How to Complete 6C paperwork checklist	Oct-03 personnel folder-clearance stuff- complete_6c_paperwork_checklist	This is a guide to properly complete the 6C clearance paperwork.
	How to Complete 5C paperwork checklist	Oct-03 personnel folder-clearance stuff- complete_5c_paperwork_checklist	This is a guide to properly complete the 5C clearance paperwork.
	How to Complete 1C paperwork checklist	Oct-03 personnel folder-clearance stuff- complete_1c_paperwork_checklist	This is a guide to properly complete the 1C clearance paperwork.
SSO Assignment Letter	Template SSO Assignment Letter	Oct-03 personnel folder- sso_assignment_letter_template	This is a template for the SSO Assignment letter. Replace the example information as needed.

New Employee or Contractor Checklist	New Employee/Contractor Checklist	Oct-03 Personnel folder- new_employee_checklist	This is a checklist for new employees/contractors of activities that they MUST complete when they join FSA.
Departing Employee or Contractor Checklist	Departing Employee/Contractor Checklist	Personnel folder- departing_employee_checklist	This is a checklist for SSOs to use that lists activities that MUST be completed when employees/contractors leave FSA.
Security Debriefing	Security Debriefing	Oct-03 personnel folder- security_debriefing	This document describes the steps an employee takes for the security debriefing process.
Contacts	Jill Mossman (hyperlink to email to jill.mossman@ed.gov)		

Organization Definition	Document	Date	Location	Description
				While it is important to have a strong security program, it is only as strong as the people that are responsible for it. In order to comply with their security obligations, individuals must know what is expected of them. The Security Roles and Responsibilities document maps the responsibilities to job titles.

Federal
NIST
ED
FSA

Security Roles and Responsibilities

Sep-03 Roles and responsibilities folder-security_roles_and_responsibilities_sept2003

This document is a one-stop reference manual for employees that addresses security responsibilities for different job roles.

Tools

For More Info

Training

Contacts

Jill Mossman
([hyperlink to email to jill.mossman@ed.gov](mailto:jill.mossman@ed.gov))

Document Title	Date	Location	Description
NIST Documents			
NIST 800-18 Guide for Developing Security Plans for Information Technology Systems	Dec-98	http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.doc	This document from the National Institute of Standards and Technology (NIST) is a Special Publication (SP) from the 800 series. This publication details the specific controls that should be documented in a system security plan.
NIST 800-26 Security Self-Assessment Guide for Information Technology Systems	1-Nov	http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf	This document from the National Institute of Standards and Technology (NIST) is a Special Publication (SP) document. This document provides a method for agency officials to determine the current status of their information technology security programs and where necessary, establish a target for improvement. This self-assessment guide utilizes an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems can be tested and measured.
NIST 800-34 Contingency Planning Guide for Information Technology Systems	Jun-02	http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf	This document from the National Institute of Standards and Technology (NIST) is a Special Publication (SP) from the 800 series. NIST Special Publication 800-34, Contingency Planning Guide for Information Technology (IT) Systems provides instructions, recommendations, and considerations for government IT contingency planning.
NIST 800-35 Guide to Information Technology Security Services	Oct-03	http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf	More agencies are contracting out for security services that support their products and programs. Special Publication 800-35, "Guide to Information Technology Security Services," outlines a life cycle for these buying services -- from determining whether a service can help in the first place all the way to ending it. The guide details the pros and cons of possibilities instead of prescribing a specific way to go about dealing with issues.

NIST 800-36 Guide to Selection Information Security Products	http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf Oct-03	Special Publication 800-36, "Guide to Selecting Information Security Products," looks at product evaluation -- an area of security receiving increased attention from Congress. It reviews potential issues for many types of products, including identification and authorization, firewalls, vulnerability scanners and forensics. It highlights the Common Criteria Evaluation and Validation Scheme, an international standard for evaluating security products now required for defense and national security and being considered for civilian agencies. The National Information Assurance Partnership, a joint venture between NIST and the National Security Agency, oversees the Common Criteria for the United States.
NIST 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems	http://csrc.nist.gov/sec-cert/ 6/1/03	This NIST document provides guidelines for certifying and accrediting federal information systems.
NIST 800-42 Guideline on Security Network Testing	http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf 10/1/03	Special Publication 800-42, "Guideline on Network Security Testing," is meant for information technology and security officials in an agency. It focuses on the details of setting up, maintaining and acting on standard enterprise network penetration testing programs. Constant testing is a major component of a security program, highlighted first by the Government Information Security Reform Act (GISRA) of 2000, and now FISMA.
NIST 800-47 Security Guide for Interconnecting Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf Aug-02	The Security Guide for Interconnecting Information Technology Systems provides guidance for planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations.
NIST 800-50 Building an Information Technology Security Awareness and Training Program	http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf Oct-03	Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program," identifies four critical steps for training and awareness -- from assessing agency wide needs to post-implementation feedback and adjustment.
NIST 800-64 Security Considerations in the Information System Development Life Cycle	http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf Oct-03	The high-level view in Special Publication 800-64, "Security Considerations in the Information System Development Life Cycle," addresses many key concerns from OMB. For years, officials have pushed agencies to consider security from the very beginning of the development of any system or program in order to head off potential incidents and save money later. Including security in the business case for any new system is now a key evaluation factor for determining whether OMB will grant agency budget requests.

FIPS Publications	FIPS Pub 199- Standards for Security Categorization of Federal Information and Information Systems	May-03	http://csrc.nist.gov/publications/drafts/FIPS-PUB-199-ipd.pdf	FIPS Publication 199 is a set of standards that define requirements for categorizing information and information systems according to a range of risk levels (low, medium, high) based upon their confidentiality, integrity, and availability.
ED Policies/Procedures	Department of Education Information Technology Security Certification and Accreditation Program Overview	6/1/03	http://connected/do_c_img/ED%20CA%20Program%20Overview.doc	The purpose of this Certification & Accreditation (C&A) Program Overview is to provide management personnel with a "road map" that clearly describes how the Department will implement the C&A program. The plan outlines specific roles and responsibilities of each stakeholder involved in the C&A program, as well as targeting major activities and allocating responsible parties to perform those actions.
	Department of Education Information Technology Security Information Technology Security Handbook for Certification and Accreditation Procedures	2/1/03	http://connected/do_c_img/ED%20CA%20Procedures%20v6.22.doc	Individuals responsible for, or involved in, the C&A process can use these procedures as a resource to certify and accredit Department's GSSs and MAs . Beyond defining a process, this document will also address several fundamental questions related to the C&A process.
	Department of Education Information Technology Security Program Information Technology Security Test & Evaluation Guide	6/1/03	http://connected/do_c_img/ED_STE%20Guide%20v5.doc	This Security Test and Evaluation (ST&E) Guide provides an overview of the content and role of an ST&E Test Plan as it relates to Certification and Accreditation (C&A) of all of the Department's GSS and MAs . It establishes the Department's parameters and minimum standards for an ST&E, which meets the requirements of the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, and the Department's Handbook for Certification and Accreditation Procedures. Department personnel responsible for the security of GSSs and MAs should use this guide to obtain an understanding of the objectives and importance, as well as the methodology, of developing and executing an ST&E Test Plan.
	Department of Education Handbook for Information Technology Security Configuration Management Planning Procedures	5/13/03	http://connected/do_c_img/Handbook%20for%20Config%20Mgmt%20Procedures%20Final.doc	This handbook provides the Department's approach to developing a configuration management plan (CMP). The handbook provides guidance to the individuals responsible for, or involved in the configuration management (CM).

Department of Education Information Technology Security Program Information Technology Security Controls Reference Guide	Jun-03	http://connected/doc_img/ED%20Security%20Controls%20Reference%20Guide%20v5.doc	This Guide is intended to provide an overview and reference of management, operational, and technical security controls.
Department of Education, Handbook for Information Technology Security Risk Assessment Procedures	5/12/2003	http://connected/doc_img/Risk%20Assessment%20Procedures%20Final.doc	These Department issued procedures may be used by a system to: 1) perform risk assessments during all stages of the system's life cycle; 2) provide guidance to contractors responsible for developing a system in preparation for an independent risk assessment; and/or 3) understand the risk assessment reports performed by the independent risk assessor.
Department of Education, Handbook for Information Technology Security Contingency Planning Procedures	6/12/2003	http://connected/doc_img/Handbook%20for%20Contingency%20Planning%20Procedure%20Final.doc	The purpose of this document is to provide Department system owners with guidance on developing IT contingency plans for their general support systems (GSS) and major applications (MA). This procedures document will describe requirements for contingency planning and provide information on preventative controls, recovery methods, and the appropriate format for a contingency plan.
Protecting Sensitive But Unclassified Information Memo	May-03	folder-OCIO_Protecting_Sensitive_But_Unclassified_Information_memo_may2003	This memo reminds the Department of the importance of handling SBU information and references Chapter 11 in the Information Security handbook for additional information.
Description of FOIA	May-03	folder-OCIO_SBU_AttachmentA_FOIA	This document is a high level overview of FOIA and how it relates to the Privacy Act.
Principal Officer Coordinators Office	May-03	folder-OCIO_SBU_AttachmentB_Principal_Office_Coordinator_list	This document is a listing of the different Principal Office Coordinators.
Department of Education, Information Technology Security Cost Estimation Guide	Nov-02	http://connected/doc_img/sec_cost_est_guide.doc	The Information Technology Security Cost Estimation Guide is designed to help Department of Education (ED) personnel with budgeting responsibilities for IT security to estimate the level of effort and cost associated with implementing security controls. Cost estimates discussed in this guide are broken down by specific security controls, which are based on the management, operational, and technical controls in NIST 800-26.

	Department of Education, Handbook for Information Technology Security General Support Systems and Major Applications Inventory Procedures	5/21/2003	http://connected1.ed.gov/po/om/executive/print/acs_hb_ocio_9.doc	This document explains the Department's GSS and MA inventory process and how to fill out the inventory worksheet.
	Departmental Directive, Information Security Incident Handling Procedures	6/26/2003	http://connected1.ed.gov/po/om/executive/print/acs_ocio_3_107.doc	This document provides incident-response guidance and procedures to ensure appropriate and expeditious handling of information security incidents that may adversely affect the Department of Education's (Department) normal business operations. These procedures define the incident-handling process, roles and responsibilities and explain how personnel should coordinate and communicate to achieve an effective and timely response to a security incident.
	Department Directive on Contractor Access	Jun-03	http://connected1.ed.gov/po/om/executive/print/acs_om_5_101_supplement.doc	This Handbook is for use by Principal Office Executive Offices and all other personnel who are responsible for ensuring that contractor employees are appropriately screened. The Handbook furnishes guidance as well as specific requirements for Principal Offices when implementing the Department of Education's policy for "Contractor Employee Personnel Security Screenings."
FSA	FSA Information Technology Security and Privacy Policy	Oct-03	policies folder-fsa_information_security_policy_aug2003	
Regulations	OMB A-130		http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html#1	This document from the Office of Management and Budget (OMB) establishes a minimum set of controls to be included in Federal IT security programs. This Circular establishes policy for the management of Federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices.
	Privacy Act		http://connected.ed.gov/index.cfm?articleobjectid=F6CE385A-E200-4E15-B2DC2FF92FF34A77 http://www.aiprp.gov.qc.ca/publication	This is the Department's information about the Act, including their guidance and a link to the Act itself.
	E-Government Act (Public Law 107-347)	Dec-02	http://www.aiprp.gov.qc.ca/publication/pdf/getdoc%5B1%5D.pdf	This is a pdf format of the full version of the E-Gov Act. Of particular interest is Section 208, which deals with privacy impact assessments. Also important is Title II, which has all of the FISMA information.

Government Paperwork Elimination
Act (GPEA)

<http://connected/index.cfm?articleobjectid=0405704D-FB58-48D6-A356E5611AB07B> This is the Department's information about the Act, including their guidance and a link to the Act itself.

<http://connected/index.cfm?articleobjectid=0405704D-FB58-48D6-A356E5611AB07B>

[17](#)

Topic	Document	Date	location	Description
C&A	C&A System Inventory File	3/3/03	C&A Folder- C&A_System_Inven tory_File	This is a tool that can be used in C&A to organize what hardware and software is located at each facility that a system uses.
	C&A System Boundaries and Interconnections	3/3/03	C&A Folder- C&A_System_Boun daries_and_Interco nnections	This is a tool that can be used in C&A to map out all of the system interconnections that a system has. The second part is a section for describing the data flow associated with each system interconnection.
Configuration Management	Configuration Management Checklist	Jan 6 2003	configuration management folder- configuration_mngt _plan_checklist_jan 03	This checklist is a way to ensure that a system's configuration management plan meets all of the requirements of the Department.
Privacy Impact Assessment	Privacy Impact Assessment Template	Jul-03	privacy folder- privacy_impact_ass essment_template_ July2003	This is a template for a privacy impact assessment along with an explanation of when a privacy impact assessment needs to be performed.
System Interconnection Documents	FSA System Interconnection Template Explanations	Aug-03	folder	This document is a high level overview describing the different system interconnection templates and when it is appropriate to use each one.
	FSA MOU Template	Aug-03	folder	When creating a system interconnection with a system located outside of Department of Education, use the FSA Interconnection Security Agreement and the FSA Memorandum of Understanding.
	FSA Trading Partner Agreement Template	Aug-03	folder	For system interconnections between systems located within the Department of Education, use the FSA Trading Partner Agreement.
	FSA Interconnection Security Agreement Template	Aug-03	folder	When creating a system interconnection with a system located outside of Department of Education, use the FSA Interconnection Security Agreement and the FSA Memorandum of Understanding.

Contingency Planning	FSA IT Contingency Planning Checklist	Jan-03	contingency planning folder-fsa_contingency_plan_checklist_Jan2003	This document is intended to assist SSOs and contractors assess existing IT contingency plans and determine its compliance with the Department's IT Contingency Planning Guide.
Incident Response	Suspicious Event Reporting Form	Aug-03	http://connected/doc_img/Suspicious%20Event%20Report%20Form.doc	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.
Badge	Id Badge Application	Oct-03	http://fsanet/forms/administration/ed_id_card.html	
Property pass	Property Pass form	Oct-03	http://fsanet/forms/administration/prop_pass_form.doc	This form is to be used if an employee or contractor will be taking equipment in and out of the building. For example, a contractor might have a company issued laptop that they will be taking in and out of the building.
Retirement Checklist	Retirement Checklist	Oct-03	http://connected/doc_img/Risk%20Assessment%20Procedures%20Final.doc	The System Retirement Checklist is Appendix F of the Department's Risk Assessment Procedures.
Inventory Worksheet	Blank Inventory Worksheet	5/21/2003	http://connected1.ed.gov/po/om/executive/print/_Toc38164541	This is a blank inventory worksheet.
CIPP Survey	CIPP Survey	Jun-05	Critical Infrastructure Protection Program folder-Critical_Infrastructure_Protection_Program_Survey_CIPP_2003	This is a blank Critical Infrastructure Protection Program (CIPP) survey.
Personnel				

Background	Guide to Background Clearance paperwork	Oct-03 Personnel folder-clearance stuff folder-guide_to_clearance_paperwork	This is a guide to determining the job risk level of an employee or a contractor and the paperwork associated with each level.
	How to Complete 6C paperwork checklist	Oct-03 personnel folder-clearance stuff-complete_6c_paperwork_checklist	This is a guide to properly complete the 6C clearance paperwork.
	How to Complete 5C paperwork checklist	Oct-03 personnel folder-clearance stuff-complete_5c_paperwork_checklist	This is a guide to properly complete the 5C clearance paperwork.
	How to Complete 1C paperwork checklist	Oct-03 personnel folder-clearance stuff-complete_1c_paperwork_checklist	This is a guide to properly complete the 1C clearance paperwork.
SSO Assignment Letter	Template SSO Assignment Letter	Oct-03 personnel folder-sso_assignment_letter_template	This is a template for the SSO Assignment letter. Replace the example information as needed.
Rules of Behavior	Rules of Behavior Template	Oct-03 forms folder-rules_of_behavior_template	When a system is creating Rules of Behavior for their system, they can use this template as an example.

Topic	Document	Date	Location	Description
General	Security Focus		http://www.securityfocus.com	Security Focus is a single place, or community, on the internet where people and corporations can go to find security information and have security questions answered by leading authorities in the industry.
	Microsoft Security		http://www.microsoft.com/security	Best practice guides, information on security technologies, or if you just want to ensure that your system is protected against all known attacks, you will find what you need here.
	Sun		http://www.sunsolve.sun.com/pub-cgi/show.pl?target=security/sec	Sun Solve on line Security Information: The Sun Security Coordination Team investigates reports of security vulnerabilities, responds to customer inquiries about security problems with Sun software, and publishes Sun Security Bulletins.
	Open BSD Security Views		http://www.openbsd.org/security.html	Open Berkeley System Development security page for OpenBSD which lists full disclosure, audit process, Cryptography, advisories, and more
Electronic Periodicals				
	Computer Incident Advisory Capability (CIAC) Notes		http://ciac.llnl.gov/cgi-bin/cnotes	A website featuring information about computer security threats for Macs, PCs, Unix systems as well as other systems.
	ZDNet		http://www.zdnet.com/zdhelp/filters/subfilter/0,7212,6002,480,00.html	ZDNet's website with links to Security and Privacy related topics such as Security Basics, Security Tips, and Network Security.
	CyberNotes		http://www.nipc.gov/cybernotes/cybernotes.htm	Bi-weekly publication by the National Infrastructure Protection Center (NIPC) to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.
	Information Security Magazine		http://infosecuritymag.techtarget.com	An online security magazine that covers information security.