

# FSA Security Policy Matrix

Consistent with FSA Policy
Partially consistent with FSA Policy; Gaps exist
ED Policy and FSA Policy conflict

2.1 Risk Management			
	<i>SFA Guide</i>	<i>ED Policy</i>	<i>Resolution Recommendation</i>
Term Definition	Risk Management is the identification, control, and minimization or elimination of security risks within an acceptable cost.		
Assess Risk and Acceptable Level	Each SFA program official shall assess the risk to systems under their control and determine the acceptable level of risk.	Each PO operating automated systems that process, transmit, or store sensitive information will establish a program for conducting periodic risk analyses for each of their AIS and IT installations. (30)	This policy does not include determination of an acceptable level of risk.
Document Risk Determinations	Every system shall document final risk determinations and related management approvals shall be documented and maintained on file.	Accreditation will be recorded in a letter from the DAA to the business or system manager and the DCIO/IA.	No policy gap.
Risk Assessment Definition	A risk assessment is an assessment of threats and vulnerabilities of information and information processing facilities, the likelihood of their occurrence, and the impact to the organization	Formal risk assessments for Department IT systems and resources may be tailored, to the system's criticality and level of the threat, in consultation with the DCIO/IA. Specific guidance is available in the Risk Management Program Guide.(30)	No policy gap.
Content of Assessment	The risk assessment shall consist of a documented analysis defining the vulnerabilities, threat sources (both natural and manmade), system flaws and weaknesses, and effectiveness of current or proposed safeguards required to lower potential loss.	A satisfactory risk assessment will consist of a fully documented, formal analysis identifying and defining the vulnerabilities and threats and recommending the safeguards required to lower potential loss to an acceptable level. (31)	No policy gap.
Content of Assessment	Each risk assessment shall include the date the system risk assessment was completed.		This policy is not addressed in Ed policy.
When to Conduct Assessment	Every system shall perform a risk assessment before the approval of design specifications for new systems.	A risk analysis will be performed before the approval of the design specifications for a new system or installation. (31)	No policy gap.

2.1.1.e Assessment due to Major Change	Every system shall perform a risk assessment and documented each time a major change occurs to the system, facilities, or other conditions.	A risk analysis will be performed whenever a significant change occurs to the system or installation. (31)	No policy gap.
Number Years Until Assessment	Every system shall perform a risk assessment a minimum of every three years.	A risk analysis will be performed at periodic intervals commensurate with the sensitivity of the information but not to exceed 5 years. (31)	SFA conducts risk assessments more frequently.
Assessment due to System Processing	Every system shall conduct a risk assessment prior to authorizing a system for processing.	Sensitive information will not be processed or stored on a Department AIS until a risk analysis has been performed or scheduled for the system or installation.	No policy gap.
Sensitivity Analysis Definition	An analysis of the criticality, sensitivity, and integrity of the information handled by each SFA system shall be described.		This policy is not addressed in Ed policy.
Content of Sensitivity Analysis	The sensitivity analysis shall contain both a general description of sensitivity and a list of applicable laws, regulations, and policies that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.		Sensitivity assessments are not required under Ed policy.
Privacy Act Systems	If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act systems of records and whether the systems are used for computer matching activities.		This policy is not addressed in Ed policy.
Protection Requirement in Sensitivity Analysis	In the sensitivity analysis, indicate if the protection requirement is high, medium, or low for each of the following three categories: confidentiality, integrity, and availability.		This policy is not addressed in Ed policy.
Business Impact Analysis	Every system shall conduct a mission/business impact analysis prior to implementing findings of the risk assessment.		This policy is not addressed in Ed policy.
Consequence Assessment	Every system shall conduct a consequence assessment, which estimates the degree of harm or loss that could occur prior to implementing findings of the risk assessment.		The topic of consequence assessment is not addressed in Ed policies.
Countermeasure Analysis	With input from SFA managers, every system shall conduct a countermeasure analysis, which determines whether the security requirements in place adequately mitigate vulnerabilities.		The topic of countermeasure analysis is not addressed in Ed policies.

Cost/Benefit Analysis	A cost benefit analysis shall be conducted to support decisions on the most cost-effective countermeasures to security risk.	Economic (cost benefit) analyses submitted by the PO business managers, to be reviewed by the PO Computer Security Officer (CSO), will support decisions as to the most cost-effective countermeasures to reduce security risks. (4)	No policy gap.
<b>2.2 Security Control Reviews</b>			
	<b>SFA Guide</b>	<b>ED Policy</b>	<b>Resolution Recommendation</b>
Periodic Review of Controls	Every system shall perform an independent review of security controls at minimum every three years or every time a significant change occurs.	Every existing or newly-developed IT system will have an OMB Circular A-130 based security review performed at least every 3 years or when a major change has occurred with the system.(37)	No policy gap.
Review System	Every system shall conduct a periodic review of the operating system to ensure the configuration prevents circumvention of the security software and application controls.	These evaluations will include those that are periodically conducted in accordance with OMB Circulars A-130, A-123 and A-127. (30)	No policy gap.
Document Reviews and Deficiencies for A-130	Every system shall document description of the type of review and findings, including information about the last independent audit or review of system and who conducted the review. An indication shall be made if the review identified a deficiency reportable under OMB A-123 or the Federal Managers' Financial Integrity Act if there is no assignment of security responsibility, no security plan, or no authorization to process for a system.	These evaluations will include those that are periodically conducted in accordance with OMB Circulars A-130, A-123 and A-127. (30)	No policy gap.
NIST Self-Assessment Requirements	Every system shall conduct a routine self-assessment every three years.		This policy is not addressed in Ed policy.
Corrective Action Plans	Management shall discuss findings and recommendations of the Corrective Action Plan, including information concerning correction of deficiencies or completion of recommendations, and ensure that significant weaknesses have been reported and corrective actions are effectively implemented.	The head of the PO will establish follow-up mechanisms to ensure that security enhancements required and approved as the result of risk assessments are properly installed and implemented in a timely manner. (31)	No policy gap.
<b>2.3 System Security Plan</b>			
	<b>SFA Guide</b>	<b>ED Policy</b>	<b>Resolution Recommendation</b>

Content	The system security plan shall discuss the system and its relationship with all interconnected systems, and contain the topics prescribed in NIST Special Publications 800-18.		This policy is not addressed in Ed policy.
General Policy	The system security plan shall be developed, updated, reviewed, and adjusted periodically to reflect current conditions and risks.	Business or functional managers are responsible for ensuring a system security plan is developed, implemented and maintained for each system supporting his or her business function, and submitting the security plan, and subsequent updates, to the DCIO/IA for review	No clear policy exists requiring security plans for every system; instead, various people are sited as being responsible for ensuring as security plan is created.
Configuration Management	Security plans should be dated for ease of tracking modifications and approvals.		This policy is not addressed in Ed policy.
Document Control	Security plans should be marked, handled, and controlled to a determined level of sensitivity.	Department personnel will ensure that sensitive materials are marked according to applicable regulations and guidance provided in Handbook #12. Appropriate marking and annotation are required for printed information, listings, diskettes and jackets, and storage devices. Appropriate preprinted labels, where possible, will be used for standardization. All media containing sensitive information must display the message "Contains Sensitive Information" externally in a clear and recognizable format. (17)	No policy gap.
Enterprise Policy	A summary of the plan shall be incorporated into the strategic IRM plan.		This policy is not addressed in Ed policy.
Enterprise Policy	Security controls shall be consistent with and an integral part of IT architecture of the agency.		This policy is not addressed in Ed policy.
<b>2.4 Rules of Behavior</b>			
	<b>SFA Guide</b>	<b>ED Policy</b>	<b>Resolution Recommendation</b>
Rules of Behavior Scope	Rules of Behavior shall reflect administrative and technical security controls in the system.		
General Policy	The Rules of Behavior shall be made available to every user prior to receiving authorization for access to the system, and it is recommended that the document contain a signature page for each user to acknowledge receipt.		This policy is not addressed in Ed policy.

Purpose of Rules	A set of rules of behavior shall be established for each system by managers at all levels to control access to, and use of equipment that permits access to any SFA system.	The business manager will have centralized responsibility for the maintenance, establishment, and enforcement of the computer security policy for all IT supporting systems within their PO or business component.(8) Managers and supervisors will 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.(17)	ED policy does not specifically identify the requirement for rules of behavior.
User Responsibilities	The Rules of Behavior shall clearly delineate responsibilities and expected behavior of system users, and hold users responsible for their own actions by stating consequences of inconsistent behavior of noncompliance.	All users are expected to understand and comply with this policy document and its requirements. Questions about the policy should be directed to the appropriate CSO or the DCIO/IA. <b>All users will report security problems or incidents to their respective SSOs or other appropriate security official. Violations of security policies may lead to revocation of system access or disciplinary action up to and including termination. (13)</b>	No policy gap.
Termination Guidance	The Rules of Behavior shall contain termination procedures for a friendly and unfriendly termination.		This policy is not addressed in Ed policy.
Differentiation of Enforcement	Differentiation should be made between rules that must always be enforced versus rules that are conditional or optional, and guidelines that express what is forbidden unless expressly authorized versus what is permitted unless expressly forbidden.		This policy is not addressed in Ed policy.
	The Rules of Behavior shall state that terminals will not be left unattended or unsecured while connected to a network.	All Department microcomputers, workstations and dedicated terminals will not be left unattended or unsecured while logged on. (23)	No policy gap.
Clear Desk and Clear Screen Policy	The Rules of Behavior shall state that sensitive media must be locked away when not in use, and computers and terminals should not be left logged on while unattended (Clear Desk and Clear Screen Policy).	Media used to record and store sensitive software or information will be protected, controlled, and secured when not in actual use.(17) All Department microcomputers, workstations and dedicated terminals will not be left unattended or unsecured while logged on. (23)	No policy gap.
Adherence to Licensing Laws	The Rules of Behavior shall state that users must abide by software licensing laws, and will prohibit the use of unauthorized software.	The use of unlicensed software is prohibited. Use of software in a manner that is not consistent with the vendor's license is strictly forbidden. (21)	No policy gap.

	The Rules of Behavior shall state that individual modems are not allowed on departmental PCs connected to the network.	The general policy of the Department is that <b>individual modems (both internally and externally mounted) are prohibited on Department networked office PCs and MACs.</b> For special purposes, those seeking a waiver must submit the justification in writing to the DCIO/IA. (23)	No policy gap.
Limitation of Connections	The Rules of Behavior shall include (a) appropriate limits on interconnections to other systems and (b) define service provision and restoration priorities, including matters such as (c) work at home, (d) dial-in access, (e) connection to Internet, (f) use of copyrighted works, (g) unofficial use of government equipment, (h) the assignment and limitation of system privileges, and (i) individual accountability.	Due to the large number of topics covered, this limited amount of space will cover the references in the Ed policy where more information can be found for each topic. (a) Section 3.4.3 Network Services, pg 19 (b) (c) (d) Section 3.4.6 Dial-In Security, pg 20 (e) Section 3.4 Network Security and the parts within the section, pg 18 (f) Section 3.4.7 Internet and Intranet Security, pg 18 (g) Section 3.17 Fraud, Waste, and Abuse, pg 34 (h) Section 3.7.1 Discretionary Access Control, pg 24 (i) Section 3.17 Fraud, Waste, and Abuse, pg 34	No policies for (b) defining service provisions and restoration priorities and (c) working at home in Ed policy.
Password Management	The Rules of Behavior will include guidance on password selection and usage, including requirements that passwords should be kept confidential, not shared, not be recycled, not based on easily guessed information, not recorded on paper at their desk, etc.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, <i>Password Usage</i> , are the minimum standards for the Department and will be fully implemented. A PO, as warranted, may establish more stringent standards for password system design, operation, and management.(23)	No policy gap.
<b>2.5 Solution Life Cycle</b>			
	<b>SFA Guide</b>	<b>ED Policy</b>	<b>Resolution Recommendation</b>
	All SFA systems shall follow the SFA SLC methodology for security.	The Department has an established System Life Cycle Management program, which presents a structured, disciplined approach to the application of IT in meeting information management needs. (27)	No policy gap.

Determine System Status	A status shall be indicated for each system, chosen from the following: Operational (system is operating), Under development (the system is being designed, developed, or implemented), Undergoing a major modification (the system is undergoing a major conversion or transition. (If more than one status is selected, list the part of the system covered under each). If a system is under development or undergoing a major modification, methods shall be provided to assure upfront security requirements.	The methodology defines a broad range of activities, starting with initial problem identification, progressing through solution development and implementation, and ending with the final disposition of the solution when it reaches the end of its useful life. In each of the following phases of this process, information security issues must be addressed to ensure that robust and cost-effective security controls are designed and built into each system. (27)	No policy gap.
Security Vision	Detailed security objectives for the system shall be defined.	The primary security focus in the definition phase of the system life cycle is to identify the detailed security objectives for the system. (27)	No policy gap.
Business Case	The budget request shall include the security resources required for the system. The Investment Review Board shall ensure any investment request includes needed security requests.		The requirement for budget request information that includes security resources is not included in Ed policy.
Resources Required	The business case shall document the resources required for adequately securing the system.		A business case is not required under the Ed policy.
	Capacity demands and projections shall be taken into consideration in order to reduce the threat of system overloading and the subsequent inability to support user services.		This topic is not addressed in Ed policy.
	The following terms shall be considered for inclusion in a contract or statement of work: asset protection; target level of service and unacceptable levels of service; liability of the contracted parties; access control agreements; the rights to monitor user activity, revoke user access, and audit contractual responsibility; the reporting structure and reporting format; involvement with subcontractors; controls to be used against malicious software; and arrangements for reporting and investigating security incidents.		This topic is not addressed in Ed policy.
<b>2.5.3 Definition</b>			
2.5.3.1 Sensitivity Assessment	Every system shall perform sensitivity assessment of the system.		Sensitivity assessments are not required under Ed policy. Also, Ed policy does not define sensitivity in terms of confidentiality, integrity and availability in the Terms and Definitions section.

2.5.2.2 Security Requirements	Security requirements of the system must be identified and defined, and a determination of each security measure shall be implemented and tested.	Owners of <i>sensitive information or systems</i> will define security requirements, based on this policy document and will approve all security specifications before the start of system development. (36)	No policy gap.
<b>2.5.4 Construction</b>			
2.5.4.1 RFP Requirements	Requirements in the solicitation documents shall permit updating security controls as new threats/vulnerabilities and as new technologies are implemented.		This topic is not addressed in Ed policy.
2.5.4.2 Testing Procedures	Appropriate security controls with associated evaluation and test procedures shall be developed before the procurement action.	The primary security concern in this [Project Request] phase is developing a security management approach, based upon the expected sensitivity of the information to be processed by the system. (27) The primary security activity during this [System Concept] phase is to identify the security requirements of the proposed system. (27)	Test/evaluation procedures are not required to be developed before procurement.
2.5.4.3 Security Requirements	Security requirements shall be identified during system design.	The primary security considerations in this [Design] phase are to determine how each security measure will be implemented and tested, to update security documentation, and to conduct design reviews. (27)	No policy gap.
	The solicitation documents (RFPs) shall include security requirements and evaluation/test procedures.	The Department will ensure that appropriate security requirements are included in all solicitations and contracts for the acquisition, operation, or significant use of AISs, or for the performance of other information-related services. (14)	Test/evaluation procedures are not required to be included in solicitation documents.
	If this is a purchased commercial application or the application contains commercial, off-the-shelf components, security requirements shall be identified and included in the acquisition specifications.		This topic is not addressed in Ed policy.
	A description of any specifications that were used and whether they are being maintained must be included.		This topic is not addressed in Ed policy.
2.5.4.4 Risk	Every system shall perform an initial risk assessment to determine security requirements.	Sensitive information will not be processed or stored on a Department AIS until a risk analysis has been performed or scheduled for the system or installation. (30) A satisfactory risk assessment will consist of a fully documented, formal analysis identifying and defining the vulnerabilities and threats and recommending the safeguards required to lower potential loss to an acceptable level. (31)	No policy gap.

	A written agreement with program officials on the countermeasures employed and residual risk shall exist.	DAA responsibilities include... reviewing and approving security safeguards; accepting, in writing, residual risk; and issuing a statement accrediting each IT system based on the effectiveness and efficiency of its design and security safeguards. (8)	No policy gap.
<b>2.5.5 Deployment</b>			
2.5.5.1 Certification and Accreditation	Every system shall request written authorization prior to operation either on an interim basis with planned corrective action or full authorization.	Sensitive and mission critical Department IT systems will only be accredited by the appointed PO DAA that the system will support and must have the written concurrence of the Department CIO before going operational. (37)	No policy gap.
	The certification testing of security controls must be conducted and documented.	Each system will undergo independent security validation and verification testing under the direction of the CSO, to evaluate the effectiveness of the system's security mechanisms. (36)	No policy gap.
2.5.5.2 Configuration Management	Changes shall be controlled as programs progress through testing to final approval.	A Configuration Control Board (CCB) will be formed within each PO to process, evaluate, and recommend approval or disapproval of proposed system configuration changes. (28)	No policy gap.
	The application shall undergo a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards.	Certification is intended to provide assurance that the system meets all applicable federal and Department policies, regulations, and standards and that the results of tests performed demonstrate that the installed security safeguards are appropriate for the system. (35)	No policy gap.
2.5.5.3 Security Awareness	Implementing and testing security measures, including security awareness training for all personnel with security and control responsibilities, shall be completed.	Each system will undergo independent security validation and verification testing under the direction of the CSO, to evaluate the effectiveness of the system's security mechanisms. (36) All individuals performing or designated to perform IT security roles will receive basic and system-specific training commensurate with assigned duties and responsibilities. (34)	No policy gap.
2.5.5.4 Post-acceptance Security Controls	If new security controls were added to the application or support system, additional acceptance tests of any new controls shall be performed, system documentation shall be updated, the security controls shall be tested, and the system shall be recertified.		This topic is not addressed in Ed policy.
2.5.5.5 Design Reviews and System Tests	Results of the design reviews and systems tests, when they were conducted, and who conducted them, should be fully documented, updated, and maintained in the organization records.		This topic is not addressed in Ed policy.

	Design reviews and systems tests shall be performed prior to placing the system into operation to assure it meets security specifications.	The system is reviewed formally to determine whether it is operating correctly and efficiently from a technical standpoint, whether it continues to meet users' information management needs from a business standpoint, and whether it is well-managed from a resource utilization perspective. Security reviews are integral components of these system reviews. (28)	No policy gap.
	If operational information is to be used during testing, a separate authorization is required each time the information is to be copied into the test application system. After testing is complete, all operational information shall be erased from the test application system.		This topic is not addressed in Ed policy.
<b>2.5.6 Support</b>			
2.5.6.1 Audits and Reviews	Security measurements inherent in the system shall be monitored through audit and periodic reviews. Audits and monitoring shall be described.	Every existing or newly-developed IT system will have an OMB Circular A-130 based security review performed at least every 3 years or when a major change has occurred with the system. (37)	No policy gap.
	It shall be determined whether the system is operating correctly from a technical standpoint, whether it meets users' information management needs from a business standpoint, and whether it is well-managed from a resource utilization perspective.	The system is reviewed formally to determine whether it is operating correctly and efficiently from a technical standpoint, whether it continues to meet users' information management needs from a business standpoint, and whether it is well-managed from a resource utilization perspective. (28)	No policy gap.
2.5.6.2 Security Plan	The system security plan shall be developed, approved, and kept current.	[Business or Functional Managers are responsible for] Ensuring a system security plan is developed, implemented and maintained for each system supporting his or her business function, and submitting the security plan, and subsequent updates, to the DCIO/IA for review. (9)	No policy gap.
2.5.6.3 Security Operations	Security operations and administration shall be described.	Roles and responsibilities for those associated with the security program are described in section 2.2. (5)	No policy gap.
<b>2.5.7 Retirement</b>			
2.5.7.1 Information Disposal	Every system shall describe the methods of how information or media is purged, overwritten, degaussed, or destroyed and how media sanitization is destroyed.	Procedures for destruction of media containing sensitive information are provided in Handbook #12. (17)	No policy gap.
2.5.7.2 Information Archival	Official electronic records shall be properly archived.		Archival information is not included in Ed policy.
<b>2.6 Certification and Accrediation</b>			
	<b>SFA Guide</b>	<b>ED Policy</b>	<b>Resolution Recommendation</b>

2.6.1	Prior to initial system operation, system/application shall be certified and accredited.	All <i>newly developed</i> Mission Essential and Mission Supportive IT systems that process sensitive information will receive accreditation before being placed in operational status.(37) Sensitive and mission critical Department IT systems will only be accredited by the appointed PO DAA that the system will support and must have the written concurrence of the Department CIO before going operational.(37)	No policy gap.
	In-place safeguards shall be operating as intended prior to authorizing a system for processing.	Based on the documented results of the design reviews and system tests, the CSO, SSO and the business manager for the system will certify that the system meets all applicable Government-wide and Department policies, regulations, and standards for the sensitivity of the system being certified and that the test results demonstrate that the specified security safeguards are in place and adequate. (36)	No policy gap.
2.6.3	A technical and/or security evaluation shall be completed prior to authorizing a system for processing.	A sensitive system shall undergo rigorous design reviews and tests by the SSO before it is placed in operation to ensure that all security requirements have been fully satisfied. Each system will undergo independent security validation and verification testing under the direction of the CSO, to evaluate the effectiveness of the system's security mechanisms. The results of this testing will be documented and included in the accreditation package. (36)	No policy gap.
	Every system shall meet all applicable federal laws, regulations, policies, guidelines, and standards.	Certification is intended to provide assurance that the system meets all applicable federal and Department policies, regulations, and standards and that the results of tests performed demonstrate that the installed security safeguards are appropriate for the system. (35)	No policy gap.
2.6.5	An IATO may be obtained for a period not to exceed 6 months when the following has been met: (1)A Full Risk Assessment (2)Security Plan (Draft) (3)Project Plan for Full Accreditation.	Conditional accreditation will be for a limited period determined by the DAA and/or the Department CIO, not to exceed 1 year, during which time the business manager must take the action to reduce the residual risk identified in the accreditation letter. (38)	ED policy does not specify minimum requirements needed to obtain IATO; ED IATO may last up to 1 year vs. 6 months at SFA.

Update Requirement	All systems shall be recertified every 3 years or upon major modification.	Sensitive applications will be recertified when substantial changes are made to the application, no more than three years have passed from the date of the previous certification. (36) Every existing or newly-developed IT system will have an OMB Circular A-130 based security review performed at least every 3 years or when a major change has occurred with the system. (37)	No policy gap.
2.6.7	Refer to SFA's C&A program manual for guidance and procedures.	Specific guidance on certification and accreditation activities within the Department are provided in the <i>Certification and Accreditation</i> Guidance document. (35)	No policy gap.
	Accreditation is recorded in a letter from the DAA to the business or system manager.	Accreditation will be recorded in a letter from the DAA to the business or system manager and the DCIO/IA.(37)	No policy gap.
2.6.9	If a system is post-IOC, and has not been certified and accredited, the system owner shall create a plan to obtain C&A.	All <i>existing</i> Mission Essential and Mission Supportive IT systems that process sensitive information will be accredited within 24 months of the date of this policy. (37)	No policy gap.
<b>2.7 Security Awareness and Training</b>			
	<b>SFA Guide</b>	<b>ED Policy</b>	<b>Resolution Recommendation</b>
	Each SFA employee shall receive a copy of the rules of behavior, which forms the basis for security awareness and training.		ED policy does not discuss Rules of Behavior
2.7.1 Training	Computer Security Awareness training shall occur within 30 days of employment and must comply with the Computer Security Act and NIST 800-16. (ED policy says it must occur within 6 months of employment within ED)	The Department's IT Security Awareness Program begins with the employee attending a suitable awareness briefing within 30 days of employment with the Department. The content, frequency, and documentation of these briefings must meet the requirements of the Computer Security Act and follow the guidance of National Institute of Standards and Technology (NIST) Special Publication 800-16. (33)	No policy gap.
	Procedures shall be set in place to ensure that each employee receives adequate training to fulfill their security responsibilities. Employee training type and frequency should be documented and monitored.	Business managers will ensure that each individual user under their cognizance receives the level of IT security awareness training commensurate with assigned duties. (33) All individuals performing or designated to perform IT security roles will receive basic and system-specific training commensurate with assigned duties and responsibilities and obtain annual refresher training to maintain their skills and proficiencies. (34)	The policy does not include mention of monitoring or documentation.

<b>2.7.2 Refresher Training</b>	Mandatory annual refresher training shall ensure that personnel remain abreast of current issues and concerns.	The Department's IT Security Awareness and Training Program will provide periodic computer security refresher briefings. These briefings will provide adequate information to ensure that personnel are kept abreast of current issues and concerns. (34)	No policy gap.
<b>2.7.3 Awareness</b>	Methods shall be employed to make employees aware of system security.	The Security Awareness and Training Work Group of the Information and Critical Infrastructure Assurance Steering Committee, in conjunction with the Department's Training and Development Group (TDG), is responsible for developing and ensuring the delivery of appropriate training curricula. (33)	No policy gap.
	Awareness briefings shall meet the requirements of the Computer Security Act and NIST 800-16.	The content, frequency, and documentation of these briefings must meet the requirements of the Computer Security Act and follow the guidance of National Institute of Standards and Technology (NIST) Special Publication 800-16, <i>Information Technology Security Training Requirements: A Role- and Performance-based Model</i> , April 1998. (34)	No policy gap.
<b>2.7.4 Contractor</b>	SFA contractor employees shall receive the same level of security awareness and training as federal employees, and this training requirement shall be included, as appropriate, in all contracts.	Initial awareness indoctrination and annual security awareness updates will be provided to all government and contractor personnel who access, manage, or use Department IT resources. Government employees and contractors will receive initial and periodic security awareness briefing(s) specific to the system(s) they use in the course of their duties. (33)	No policy gap.
	Computer Security Awareness training shall occur within 30 days of contract award.	Contractor employees must be briefed within 30 days of assignment to a Department contract. (34)	No policy gap.
<b>2.8 System Interconnections</b>			
	<b>SFA Guide</b>	<b>ED Policy</b>	<b>Resolution Recommendation</b>
	System interconnections are not allowed unless expressly documented in an MOU/MOA/SLA.	IT systems or applications connected to the Department's network require a Memorandum of Agreement (MOA). (19)	No policy gap.
Interconnecting System Authorization	Written authorization shall detail the rules of behavior and controls that must be maintained by the interconnecting systems.	This topic is discussed in Section 3.4 Network Security. (18)	No policy gap.

	Written management authorization shall be obtained prior to connecting with other systems and/or sharing sensitive data/information (OMB A-130), including a list of interconnected systems (including Internet).	IT systems or applications connected to the Department's network require a Memorandum of Agreement (MOA) between the system DAA (or application owner) and the Department DAA, which will provide assurances that appropriate security controls have been implemented. The MOA will be reviewed and validated by both parties and signed by the appropriate senior officials who may include the DAA's, DCIO/IA and or the CIO. (19)	No policy gap.
	Every system shall document whether or not the application is processed at a facility outside of the organization's control.		This topic was not mentioned in the Ed policy.
Outsourced Contract Requirements	Outsourced contracts shall include: how legal requirements are met; physical and logical controls to be used to restrict and limit access to sensitive information to only authorized users; the expected availability of services to be maintained in the event of a disaster; levels of physical security for outsourced equipment; and the right to audit.	The SSO in conjunction with the CSO will ensure that all appropriate security requirements are included in all statements of work and that appropriate risk levels are assigned to each position in accordance with Section 3.2 of this document, and Handbook #11. (14)	Topics not included in Ed Policy are: how legal requirements are met; physical and logical controls to be used to restrict and limit access to sensitive information to only authorized users; the expected availability of services to be maintained in the event of a disaster; levels of physical security for outsourced equipment; and the right to audit.