



Office of Student Financial Assistance

Risk Assessment Report

**An Evaluation of the SFA Systems
Security and Privacy Risk Management and Control Environment
With Recommendations for Improvement**

Prepared by:



August 31, 2000

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

BACKGROUND 5

TASK OVERVIEW 5
REPORT OVERVIEW 6
SYSTEMS OVERVIEW 6

DISCUSSION 13

THE CASE FOR IMPLEMENTING THE GAO RISK MANAGEMENT CYCLE..... 13
CONTROL ENVIRONMENT OBSERVATIONS 15

CONCLUSIONS 100

RECOMMENDATIONS 101

Executive Summary

KPMG evaluated the risks to several Office of Student Financial Assistance (SFA) systems that support SFA's core business process. Specifically, these systems process and store information for the disbursement and financial management of student aid appropriations.

To accomplish this task, KPMG security analysts and engineers collected information on SFA systems, network architectures, operations, the physical environment where hardware is located, data elements and business processes. The approach used to gather this information included inquiries to SFA management, staff and information technology contractors, documentation review, and review of responses to a security and privacy survey developed and distributed by KPMG. The information was then analyzed to evaluate the maturity of SFA's risk management model and to determine how well that model was being applied at the system level for those systems in the scope of this project.

The standard used to measure the maturity of SFA risk management was derived from guidance provided by the General Accounting Office (GAO), summarized below in Figure 1; security and privacy standards contained in [Appendix I](#) and [Appendix III](#) of the Office of Management and Budget (OMB) Circular A-130; and National Institute for Standards and Technology (NIST) Special Pubs [800-14](#) and [800-18](#). This measurement guidance was developed based on the [Privacy Act of 1974](#) and the [Computer Security Act of 1987](#).

KPMG also considered how the criteria and controls could be applied to SFA's public service mission and their current business model that carries out the mission. Consistent with the guidance provided by SFA management, this project was not so much to determine how rigidly SFA was adhering to legal and regulatory guidance, but to provide insight to SFA on how the criteria could be better applied to help SFA manage the risk to its critical applications and systems.

Risk management was analyzed at both the system level and the organizational level. At the system level, we found similar opportunities for improvement across all systems. We assess the consistent system-level weaknesses as merely symptomatic of enterprise-level issues. Improvements to risk management processes at the enterprise level are likely to result in long-term benefits at the system level. This is not to imply that improvements cannot and should not be made at the system level – they can and we recommend that they should be made. But without enterprise-level risk management support, guidance and monitoring, system-level problems will tend to recur.

We conclude that the overall maturity of SFA risk management processes are immature at both the system and organizational level, and we recommend SFA take steps to strengthen every phase of the risk management cycle. In priority order, we recommend:

1. Provide security skill set training to Systems Security Officers (SSOs),
2. Develop system security plans,
3. Implement rules of behavior that are consistent across all systems,
4. Develop better, more detailed system functional and technical descriptions,

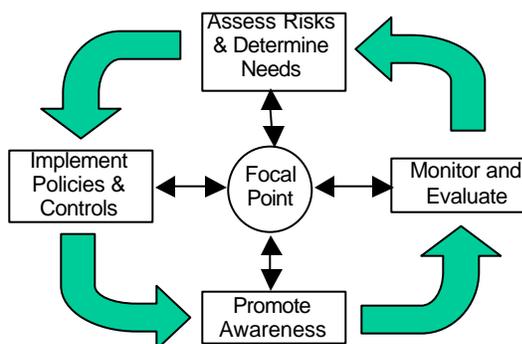


Figure 1: GAO Risk Management Cycle

5. Develop and execute an enterprise-wide security training and awareness program,
6. Develop enterprise-wide security standards,
7. Develop metrics and procedures for evaluating for high-risk security events,
8. Enable audit logs to capture information on high-risk events,
9. Subject captured data in the audit log to periodic analysis,
10. Continue to perform follow-on risk assessment using the GAO/NIST model,
11. Develop a security model that assigns information sensitivity levels and ownership, and
12. Implement a formal certification and accreditation process using FIPS 102 guidance.

Background

The Office of Student Financial Assistance (SFA) is an independent agency under the U.S. Department of Education (ED). SFA's mission is to manage disbursements of annual student aid appropriations. These appropriations are made annually by Congress.

A significant challenge SFA encounters is that the appropriation terms and conditions often change from year to year. This fact creates a dynamic environment for SFA system managers since they must continue to properly enforce current year appropriation rules of behavior, but also remain in compliance with Federal laws, regulations, and other guidance pertaining to managing information security and personal privacy risk.

In this dynamic environment, SFA must have a robust risk management process in place and operating, both to ensure public trust in SFA is not undermined and SFA compliance with applicable Federal guidance is continuously measured and enforced. The foundation for such a process must consist of:

1. A security, privacy, and risk management vision,
2. Continuous and visible executive support for this vision,
3. An enterprise-wide security/privacy training and awareness program, and
4. A security management structure with sufficient resources and authority to make the vision an operational reality.

The security, privacy and risk management yardstick has already been established for Federal entities through laws, regulations, and standards. Relevant laws include the [Privacy Act of 1974](#) and the [Computer Security Act of 1987](#). These laws are implemented through regulatory guidance as follows:

1. The Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, establishes policy. Procedural and analytic guidelines for implementing A-130 are provided in its appendices. The two appendices relevant to this task are [A-130 Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals](#), and [A-130 Appendix III, Security of Federal Automated Information Resources](#). Appendix I provides overall guidance for implementing the Privacy Act, while Appendix III provides overall guidance for implementing the Computer Security Act. Appendix III also points Federal managers to specific guidance relating to computer security that has been promulgated by the National Institute of Standards and Technology (NIST).
2. NIST has issued a trio of publications that provide highly detailed guidance for establishing a secure environment in Federal automated information systems in accordance with A-130. These are: NIST Special Pub 800-12, *Introduction to Computer Security*, [NIST Special Pub 800-14, Generally Accepted Best Practices for Securing Information Technology Systems](#), and [NIST Special Pub 800-18, Guide for Developing Security Plans for Information Technology Systems](#).

An example of a government-wide risk management process is described in General Accounting Office (GAO) report [GAO/AIMD-98-92, Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk](#), September 1998. This document describes a risk management model based on OMB and NIST policy and guidance. While OMB/NIST describe *what* to do to mitigate risks in automated information systems, the GAO risk management model describes *how* to do it.

Task overview

KPMG performed a risk assessment of nine systems used by SFA to perform and manage many of the functions related to originating, disbursing and managing student loan programs appropriated by Congress. Specifically, one system, Title IV Wide Area Network (TIV WAN) fits the description of a [general support system](#) that is designed to support the entire SFA financial assistance architecture while the other eight were developed as [major applications](#) designed to support specific SFA's business processes.

KPMG employed several methods for obtaining information. This included review of provided system documentation, previous security/control-related assessments (e.g. past A-130 reviews), and interviews and meetings with SFA OCIO, system management, security personnel, and users. However, due to the task's broad scope and aggressive schedule, security and privacy questionnaires were also developed and disseminated in order to collect specific information concerning individual systems' control environments. This method a) obviated the need to set up and conduct a large number of individual interviews, b) permitted information on nine systems to be collected in parallel rather than in serial fashion, and c) leveraged limited KPMG staff resources, and d) represented the least disruption to SFA business.

SFA management noted at the outset of the task that security for the sake of compliance was less important than security to enhance SFA's ability to protect privacy and to meet its business goals. KPMG was therefore directed to consider how the criteria and controls could be applied to SFA's current business model for carrying out its public service mission. Consistent with that guidance, this document not only measures SFA adherence to legal and regulatory guidance, but also explores how the criteria might be applied to help SFA manage the risk to its major applications and systems.

Report overview

Risk management was analyzed at the system level to identify common risks across SFA's systems and specific system risks. This report has been designed to identify both the common, organizational issues, and system-specific risks. We have also included suggested recommendations to decrease both the organizational and system risks.

Given the complexity of the systems and security standards covered in the task, this report has been constructed in such a way as to facilitate the reader's understanding. This document is intended to be viewed on-line rather than in printed form. Taking advantage of Microsoft Word's ability to build links inside and between documents, this report is best navigated through the hyperlinks built into the document, displayed as blue, underlined text. These links enable the reader to:

- Navigate the analytical portions of the document from a single [Risk Management Cycle illustration](#), shown below.
- Maneuver easily from an organizational-level view of risk management down to individual systems' risks, and back.
- Associate KPMG's suggested recommendations to related legal and regulatory guidance, and to SFA risk management and business processes.
- Quickly access pertinent source and reference documents.

Systems overview

Nine systems were examined during the course of this risk assessment task. The purpose of this section is to provide a brief functional and technical description of each system, and to describe where these systems collectively fit into the SFA business process. The surveyed systems are:

- Campus-Based System (CBS)
- Central Processing System (CPS)
- Direct Loan Central Database/Direct Loan Servicing System (DLCD/DLSS)
- Direct Loan Origination System (DLOS)
- Federal Family Education Loan System (FFEL)
- National Student Loan Data System (NSLDS)
- Pell Grant Recipient Financial Management System (RFMS or Pell)
- Postsecondary Education Participants System (PEPS)
- Title IV Wide Area Network (TIV WAN)

Descriptive documentation on individual systems varied widely; in many cases it was not possible to ascertain such things as major system functions, data inputs and outputs, and system/subsystem physical locations. In addition, while most systems' documentation included lists of hardware and software components, descriptions of the hardware and software architecture (how the hardware and software are integrated and function) were available for only a few systems.

Campus Based System (CBS)

CBS supports the College Work-Study and other small student grant programs administered at the campus level. The system supports the process through which schools apply for and receive funds from SFA's education appropriations.

The electronic application form used to apply for funds is called a Fiscal Operations Report and Application to Participate (FISAP). FISAPs are submitted annually through CBS to SFA. SFA disburses funds from various specific programs directly to the applying institutions. The schools are then responsible for further disbursement to individual students.

Major functions include:

- Processing campus-based funding
- Maintaining and editing FISAPs
- Calculating and notifying institutions of their awards
- Allocating campus-based funds
- Reconciling accounts and producing financial reports
- Support of the default reduction assistance program

Inputs to CBS include FISAPs, the CBS master file of participating institutions, database correction data, funding allocation parameters, funding calculation parameters, information service requests, certification and tracking forms, and electronic application and editing data. The most important outputs from the standpoint of financial management are the funding allocation reports that are transmitted to the Grants Administration and Payment system (GAPS), which is a subsystem of ED's principal financial management system, *Education Central Automated Processing System* (EDCAPS). Other outputs include institutional status control files, edit reports, and funding notices. Other outputs include database updates, informational reports, customized letters, microfiche files, and documents prepared for retirement to the Federal Records center.

CBS is hosted on an IBM 9672 RB5 mainframe and runs on the OS390 operating system. The database is IBM VSAM; network communications use the SNA-LU protocol. Access rights and application privileges are controlled using IBM's Resource Access Control Facility (RACF) product.

Individual institutions are provided with secure "mailboxes" on the CBS mainframe that prevent other participating schools from viewing their mailbox information. Institutions connect to their mailbox across the Title IV Wide Area Network ([TIVWAN](#)) using EDExpress (a school-based electronic application program).

The CBS mainframe is located in Meriden, CT, in the Virtual Data Center (VDC) run by CSC's Technology Management Group (TMG). The Meriden VDC is [described below](#).

Central Processing System (CPS)

CPS is a centralized system for processing applications for student financial aid from students in Title IV programs. Its primary function is to process each submitted Free Application for Federal Student Aid (FAFSA) application through a series of data checks, formula calculations and verification checks with

other Federal agencies. CPS then prints the information and eligibility results on a Student Aid Report (SAR) for mailing to the student or institution.

Other major functions include:

- Maintaining records of every application submitted for Federal student financial aid.
- Performing data information matches with:
 - 1) Federal agencies (e.g., Selective Service (SS), Immigration and Naturalization Service (INS), the Department of Justice Drug Abuse Data Base, Social Security Administration (SSA) and the General Services Administration Debarment and Suspension Program;
 - 2) The National Student Loan Data System ([NSLDS](#)); and
 - 3) The Hold File, which includes Federal Pell Grant Overpayments and other problem cases.
- Interfacing with other Federal systems, eligible institutions and students in order to perform these functions.
- Confirming applicants' eligibility for Federal student financial assistance
- Calculating the estimated family contribution (EFC)
- Calculating eligibility for Federal aid (i.e., determine financial need)
- Reporting eligibility information to applicants, schools, and guarantors
- Supporting management information and analysis requirements of other ED managers and staff.

CPS works hand-in-hand with EDEExpress, a microcomputer-based software package distributed by ED to schools to support aid packaging, Federal Pell Grant and Federal Direct Loan origination, SSCRR, and drawdown of data from CPS for use in other school applications. In addition, the CPS program office is responsible for developing, testing, and distributing the EDEExpress software, FAFSA Express software, EDE Express Tutorial software, and the Pell Payment software.

Inputs to CPS include applicant data received through Multiple Data Entry (MDE, a campus-based application), FAFSA Express, EDEExpress, and web sources. CPS can output over 100 management, analytical, and financial aid reports, however, from a financial management standpoint its most significant outputs are to the NSLDS and EDCAPS/GAPS.

CPS is hosted on an IBM 9672 RB5 mainframe and runs on the OS390 operating system. Access rights and application privileges are controlled using IBM's RACF product.

The CPS mainframe was moved recently from Iowa City, IA, to CSC's [Meriden, CT VDC](#), described below.

Direct Loan Central Database/Direct Loan Servicing System (DLCD/DLSS)

DLSS maintains data on students under the FDLP program while the students are in school, deferment, or repayment status. DLCD is a component of the Direct Loan Servicing System.

These two systems jointly are responsible for servicing all of ED's direct student loans and maintains the ledger accounts for all financial transactions associated with the program.

Direct Loan Origination System (DLOS)

DLOS is made up of two applications: the Loan Origination (LO) application and the Loan Consolidation (LC) application. The purpose of the LO Application is to process Loan Origination, Promissory Note and Disbursement data sent in by schools for award of Stafford and PLUS loans. The purpose of the LC application is to allow a borrower to consolidate their student loans. The information processed includes borrower demographic data, financial data, and student loan data.

Direct Loans are initiated at the school level (information is collected, packaged and batched at the school) and forwarded via origination records to the LOS using EDConnect or mainframe transmission and the [TIVWAN](#), also known as Student Aid Internet Gateway (SAIG). Disbursements and Change Records are initiated in the same way. Schools may create and process their records using the EDEExpress software, Third Party Servicers or a Custom (Mainframe) System of their own. For the high-level processes described in this document, SAM is treated the same as a school. Although SAM is treated the same as a school, it does not send, receive, or process promissory notes in any manner. All input sources must be processed by the LOS.

Once information has been processed for the records submitted by schools, the LOS generates an acknowledgment indicating that records have been received and processed. All records and batches submitted are edited using defined system edits available in the Direct Loan Technical Reference Custom Section. The LOS also generates the letters regarding status, and requests for information, when necessary, for designated records. These letters are sent to the borrowers and/or schools who need to provide additional information or corrections.

The Loan Origination Record (LOR) contains the demographic, financial, and statistical information necessary to create a borrower record in the Department's Direct Loan database. This information includes Anticipated Disbursement data (date and amount). The LOS receives a loan origination record from the school via the SAIG. Once the LOS receives the loan origination record, it is edited and validated. A credit check report is obtained for the borrower and/or endorser upon receipt and validation of a PLUS loan origination record or an endorser form. A credit check request is not performed on subsidized or unsubsidized loans. If a previous positive credit decision has been received by the LOC within 90 days, the previous credit decision is used and a new decision is not obtained. The credit check request is forwarded through the contractor's credit check interface system (OLNACS) to the credit agency. The credit check result is recorded in the loan origination record and acknowledged to the school on the Loan Origination Acknowledgment. Borrowers or endorsers are notified of both accepted and adverse credit results. In accordance with Department guidelines, credit results may be overridden. Rejected borrowers may appeal, in writing, citing extenuating circumstances. LOC personnel review appeals in accordance with Department guidelines and may override negative credit decisions with Department approval. In this case, a credit check override is acknowledged to the school. A "LO Extenuating Circumstance Credit Override Letter" is sent to the borrower as notification that the override appeal has been approved. If the override appeal is denied, the "LO Extenuating Circumstances Credit Override Rejection Letter" is sent to the applicant.

After a Loan Origination Record has been established for a student, a Disclosure Statement is sent to the borrower based on the anticipated disbursements reported on the Loan Origination Record. The Disclosure Statement is generated and mailed approximately 10 days prior to the first anticipated disbursement date.

LOS receives change records from a school via the TIVWAN. A change record updates the loan origination record already stored on the LOS database. For example, a change record can update demographic data, dependency status, loan amount approved, anticipated disbursements, and anticipated disbursement dates. The changes are edited and validated and, if accepted, are applied to the loan origination record already in the LOS database. All records are acknowledged to the school as accepted or rejected on the Loan Origination Change Acknowledgment.

A promissory note is generated and sent to the borrower, either by the school or the LOC, depending on the school's level/option. Level 1/Option 2 and Level 2/Option 1 schools have the option of printing their promissory notes at the school. The subsidized and unsubsidized loans are now processed with a Master Promissory Note (MPN) for each student. An MPN can be active for up to 10 years from the date of the first actual disbursement on a loan. This Master Promissory Note can be used for any additional Direct Subsidized or Unsubsidized loans the borrower may receive throughout their financial aid history. These promissory notes with multi-year functionality are called Multi-Year Notes (MYN). Although all subsidized and unsubsidized promissory notes are MPNs not all MPNs are multi-year. Only four-year institutions are eligible to participate in the multi-year functionality. PLUS loans are not eligible for multi-year functionality or the MPN. The PLUS Loans are processed on the PLUS Loan Promissory Note. The

LOC is responsible for receipt and storage of all promissory notes. Once these promissory notes are received and have passed through the editing process, the LOS is responsible for generating an acknowledgment to the schools notifying the school of receipt of the Promissory Note. Completed promissory notes received by the LOC are reviewed in accordance with Department guidelines and are imaged, indexed, and stored in a fireproof, secure vault at the LOC. An imaged copy of the Promissory Note is displayed on a terminal along with the data of the electronic promissory note record. The promissory note record is then quality checked to ensure the Optical Character Reader (OCR) was done correctly. Once the promissory note is free of errors, the electronic image is stored on the system.

All schools transmit actual disbursement records to the LOC via the TIVWAN. The LOC edits and validates actual disbursement records. A loan must be disbursed in at least two actual disbursements. However, up to twenty disbursements are allowed. There are some exception schools which are allowed to fully disburse a loan in one disbursement. If an actual disbursement record does not pass edits, it is rejected, and the school must resolve and resubmit it to the LOC. The LOC transmits a Disbursement Acknowledgment to the school, indicating all accepted and rejected disbursements. An adjusted disbursement amount record is transmitted to the LOC when the amount of a disbursement needs to be increased or decreased. This includes disbursements being adjusted to zero. An adjusted disbursement date record is transmitted to the LOC when the date of an original disbursement needs to be changed. The LOS database produces the Anticipated Disbursement Listing (ADL) and the Actual Disbursement Roster (ADR). The ADL is created 45 days prior to the date of the first anticipated disbursement reported on the LOR. Level 1/Option 2 schools estimate and perform their own draw downs based upon the ADL and their own financial records. The ADR, based on anticipated disbursements, notifies the school that the LOS requested the funds from GAPS and provides a detailed listing of the disbursements, scheduled to be made with the funds. A valid accepted and signed promissory note is necessary to make disbursements for Level 2/Option 1 and Standard option schools. A promissory note does not have to be on file at the LOC in order for the Level 1/Option 2 school to make a disbursement. Some schools which have been designated as Access America Schools send their disbursements to the LOS via the Student Account Manager (SAM).

Funds are requested from the Grants Administration and Payment System (GAPS) using the anticipated disbursement dates and anticipated disbursement amounts reported on the Loan Origination record. The request for funds or "draw downs" depends on the schools operation level. Level 1/Option 2 schools request their own draw downs. Other school options have their draw downs requested by the LOS, with the exception of Level 5 schools. The draw downs for Level 5 schools are performed by the Department. Once a drawdown has been made for a school, if the school does not disburse the funds within 3 days, the school has an Excess cash condition. Level 1/Option 2 schools may disburse this money to another student. However, if the money is not disbursed to another student it is deemed Excess Cash. All other levels/options must return the Excess Cash immediately after the 3 days. Excess Cash when returned to the LOC is processed. There are several methods for the Return of Excess Cash, ACH, Fedwire and Check. However, all methods are processed at the LOC.

Once an Origination, Promissory Note and Actual Disbursement have been processed and accepted, the loan is considered "Booked" and is ready to be forwarded to the Central Database System for continued processing.

A Loan Consolidation Application can be received via paper, web, or over the telephone. When a paper application is received it is opened, reviewed, and imaged by the mailroom. The imaged application is data entered by the Data Entry Group and sent to Exam Entry. Exam Entry reviews all applications to ensure the required information is present before it is released to Certification. Exam Entry reviews the data-entered applications, telephone applications entered directly into the system, and the applications received from the Web Application. If any information is not present, Exam Entry will contact the borrower directly. After the application is released by Exam Entry, the system generates Certifications to be sent to the loan holders to certify the payoff amount. Certifications returned by the loan holders are imaged and data entered by the Certification Group. Once all the certifications are received, a loan statement is generated and sent to the borrower for final review. Loans that meet certain criteria also go through Pnote Underwriting, which performs another check of the loan amounts. The loan is then funded and payoffs are sent to the loan

holders. Finally, the loan is booked and the required transactions are sent to the Central Database System and Direct Loan Servicing Center.

The following UNIX servers are used to support the LOS. These servers physically reside at the [Virtual Data Center \(VDC\)](#) in Meriden, Connecticut, under the management of Computer Sciences Corporation (CSC).

The LOS production server contains the LOS production database. This database is accessed during the day by CSRs at the LOC as well as by schools using the LOS Web application. Data from the TIVWAN is retrieved twice a day and feeds nightly batch processing, which also occurs on this server. Batch file transfers to CDS, OLNACS, and GAPS also occur on a nightly basis.

Users at the LOC connect to the servers at the VDC via two T1 circuits. Developers at the BDC use a frame relay connection to access the LOS servers at the VDC. Multiple T1 circuits, terminating at the VDC, are used to connect to the LOS production server with TIVWAN and GAPS. A 56kbps point-to-point circuit is used to connect with OLNACS. The LOS Web server contains the LOS Web application. The LOS development server contains the various LOS test and development environments. This server is used by developers at the BDC and LOC to develop and test new functionality to the LOS.

The LOS Web test server is used to support the development and testing of new releases of the LOS web application.

Federal Family Education Loan System (FFEL)

FFEL processes transactions related to the FFEL program including interest and special allowance payments to lenders and default claims to guaranty agencies. The FFEL Debt Collection subsystem is used to support ED collection of defaulted loans from all Title IV loan programs and to collect Federal Pell Grant overpayments.

FFEL is used to pay interest and special allowances and to pay ACA to guarantors. The Debt Collection subsystem supports ED collection of defaulted loans from all Title IV loan programs and Pell Grant overpayments.

National Student Loan Data System (NSLDS)

NSLDS is a database used to prescreen Title IV aid applications to prevent ineligible students from receiving aid. NSLDS calculates cohort default rates for schools, guaranty agencies and lenders. NSLDS allows schools and guaranty agencies access to online functions that assist them in tracking students' Title IV aid history.

Pell Grant Recipient Financial Management System (RFMS or Pell)

RFMS stores program information on post-secondary institutions and recipients participating in the Pell Grant Program. It provides fund accountability and control information and source data for program budgeting and evaluation.

Postsecondary Education Participants System (PEPS)

PEPS is a repository of eligibility, certification, address and participation data on institutions in Title IV programs. PEPS is used primarily by ED to monitor postsecondary institutions' participation within the Title IV programs. It is the official source of information on schools and school codes for all ED systems.

Title IV Wide Area Network (TIVWAN)

TIVWAN provides the network link from institutions to the Department's Title IV systems ([CBS](#), [CPS](#), [DLOS](#), [DLSS](#), [FFEL](#), [PEPS](#), and [RFMS](#)) for the delivery of student financial information.

TIVWAN acts as the conduit for information flowing between the institutions and the application systems involved with the delivery of federal student financial aid. The TIVWAN's primary role is to provide the network connections and store-and-forward mailbox system that allows post-secondary education institutions and ED's contractor systems to exchange data electronically. To do this, TIVWAN maintains a database of schools and their participation details. This information is then sent to the application systems so they can route return messages.

The Meriden Virtual Data Center

CSC's Meriden VDC is a large-scale data service center that offers over 1800 MIPS of mainframe and large server capacity, high performance disk and tape storage systems, and high volume print operations. Many of SFA's systems have been relocated from various data centers in the United States into the Meriden facility. The centralization of the systems to the Meriden facility did not result in systems being consolidated onto one shared platform; rather, the systems in existence – hardware and software – have been moved into the VDC. While SFA has long-range plans to consolidate systems and functionality, at the time of this survey the systems retain their individual, discrete architectures and are merely housed under a common roof and managed by a common operating staff.

Operated by CSC's Technology Management Group (TMG), the Meriden VDC is located on an 18-acre facility with up to 160,000 square feet of operational space available. This includes up to 80,000 square feet of raised-deck computer space; the remainder of the available space is devoted to offices, maintenance support, and facilities support.

Deloitte & Touche (D&T), LLP has performed a Statement of Auditing Standards number 70 (SAS-70) report that covers the period December 1, 1998 through November 30, 1999. A SAS-70 is commonly performed to allow interested parties such as auditors and SFA management to evaluate the sites information technology controls. Therefore, the SAS-70 is performed by an independent audit organization that serves as a trusted third-party. This independent auditor, under the service center's instructions, performs the control tests that interested parties auditors would normally perform for themselves, and provides a report to all client auditors in lieu of their controls testing.

SAS-70s are normally written to cover the same period that a financial audit covers – 12 to 18 months. After that time, the report is no longer considered a trustworthy basis for financial opinion. This is the case in the current instance; the VDC SAS-70 report is no longer useful for financial audit purposes. However as a control review it falls well within OMB A-130's recommended tri-annual control assessment criteria. For this reason, KPMG has used D&T's SAS-70 as the basis for assessing risk at the VDC.

Discussion

The Case For Implementing the GAO Risk Management Cycle

At SFA, information is not simply a by-product, it is the product itself. SFA's ability to carry out its public service mission is almost wholly dependent on protecting information privacy or confidentiality, integrity, and availability. Failure in any one of these areas can have undesirable consequences for SFA and its customers: privacy compromise, loss of ability to deliver service, or loss of reputation/customer confidence (e.g. Department of Justice Web Page hack). Because information is crucial to SFA, it is reasonable to examine what SFA is doing to mitigate the risk to its most valuable asset. As noted above, the GAO risk management model has been used as the basis for assessing risk and SFA risk management capabilities.

The GAO risk management model takes a common sense approach to managing risk. The first phase calls for deciding what the risk environment looks like for a given system and the information the system processes, stores, or transmits. Once the risk environment is understood, control measures need to be implemented to mitigate the risk to an acceptable level, and personnel have to be trained in order to understand those controls and the risk they are intended to mitigate. Management must have a means for measuring compliance and monitoring changes in the risk environment; only in this way can they make risk decisions – accept or mitigate risk on purpose.

However, risks to information cannot be eliminated entirely, but must be managed through the application of administrative, operational, technical, and physical security practices. Further, risk mitigation methodology must address information security from an enterprise-wide perspective. No single person, no single office within SFA can implement security. However, when policies, practices, and technologies are fully integrated and implemented within an enterprise-wide framework, security becomes the enabler that helps SFA become more effective and efficient in attaining its public service goals. To achieve this, organizations should implement a risk management process such as that recommended by GAO, using guidance provided by NIST.

The first key element in the GAO risk management cycle is the focal point for coordinating risk management activities. [NIST Special Pub 800-14](#) describes the need for both central and system-level focus:

“Managing computer security at multiple levels brings many benefits. Each level contributes to the overall computer security program with different types of expertise, authority, and resources. In general, executive managers (such as those at the headquarters level) better understand the organization as a whole and have more authority. On the other hand, front-line managers (at the computer facility and applications levels) are more familiar with the specific requirements, both technical and procedural, and problems of the systems and the users. The levels of computer security program management should be complementary; each can help the other be more effective. Many organizations have at least two levels of computer security management; the *central* level and the *system* level....

A central security program should provide distinct types of benefits: increased efficiency and economy of security throughout the organization and the ability to provide centralized enforcement and oversight....

While the central program addresses the entire spectrum of computer security for an organization, *system-level computer security programs* ensure appropriate and cost-effective security for each system. System-level computer security programs may address, for example, the computing resources within an operational element, a major application, or a group of similar systems (either technologically or functionally)....”

Risk management cannot be performed from the bottom up. Any asset upon which an organization chiefly depends should be the daily concern of the highest levels of management, not just the security staff. If information assurance is not a visible and consistent priority for the executive and senior managers who have authority and control resources, risk management will fail.

In addition, responsibility for risk decisions cannot be outsourced. While many SFA system management functions have been outsourced, including security implementation, allowing risk management decisions to be made by vendors is not viable due to the potential conflict of interest. History demonstrates that companies are often reluctant to point out deficiencies in their own products; SFA managers must therefore ensure mechanisms are in place to allow proactive oversight and coordination.

The second key element in the GAO cycle is assessing risks and determining needs. The risk assessment examines the organization's administrative, operational, physical, and technical environments to determine where vulnerabilities may exist. Where weaknesses are found, the process then looks for corresponding threats; where there is correlation, the risk must be assessed. Factors influencing risk at SFA include federal and industry best practices, laws and regulations, operational practices and technology use, and information sensitivity/criticality. At the enterprise level the risk assessment provides SFA management with an understanding of the adequacy of the control and risk management environment. At the system level, this knowledge can be applied by systems managers to prioritize and balance information protection needs against available resources.

The third key activity is implementing policies and controls. Once the risk environment is understood, information security policies must be put in place; in SFA's case much of this policy has been promulgated by the Department of Education. Policies are high-level statements intended to provide guidance to executive managers and other decision makers. Most importantly, policy provisions are mandatory and must not be deviated from without special approval from the policy owner. This is a critical distinction from procedures and guidelines; these may be changed (within policy bounds) as circumstances dictate.

In concert with policy, a security model is used to structure, organize, and focus security efforts. The security model provides centralized framework through which information can be classified and categorized based on sensitivity. It also defines a data ownership architecture that assists in delegating authority for control implementation throughout the organization. Further, the security model defines user information protection responsibilities.

The security model will be implemented at a macro level through operational and technical standards. The International Standards Organization (ISO) defines standards as "...documented agreements containing technical or other precise criteria to be used as rules, guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purposes." Standards establish acceptable technical minimums and maximums, define specific control standards, and identify specific products required to support the security policy and model.

At the systems level, standards are implemented through product- and user-specific procedures and guidelines. These procedures provided detailed, specific, day-to-day guidance on administrative, operational, physical, and technical processes and tasks. They include end-user guidelines that clearly articulate expectations, roles, and responsibilities. Through this guidance, risk awareness and basic security concepts, procedures and practices are reinforced with end users and operators.

The fourth key element in the GAO cycle is to promote awareness of privacy and security policies, standards and procedures throughout the operating environment. Risk Management must become fully integrated into organizational culture; managers, employees and vendors at every level must learn to integrate risk management into their every-day thinking. The only way to attain this is to provide security awareness training to all levels of organization. This training must cover all aspects of information assurance *in an SFA business context*. In addition to being pervasive, it must also be provided continuously, and made an integral part of vendor, employee and management training.

The fifth and final key activity in the GAO risk management cycle is monitoring and evaluation of the control environment. Once policies, standards, and procedures are in place, manual and automated monitoring processes to prevent and detect compromise to information confidentiality, integrity, and availability must be implemented. Monitoring includes such things as periodic real-time and retrospective transaction and activity assessment and penetration analysis. Enforcement involves proper staffing prior to the introduction of new technologies or processes to ensure innovations support business goals and policies. It also includes analysis of the output from monitoring activities to determine compliance with policies and standards, and adherence to accepted procedures. When monitoring and enforcement fail, it is critical that organizations have pre-determined recovery procedures. These might include a disaster recovery and continuity of operations plan, physical or logical intrusion response procedures, and administrative sanctions for non-compliance with policy and standards of conduct.

In the GAO model, monitoring and evaluation activities lead back to risk assessment. Risk management is not a point-in-time activity. Whatever risk management model is adopted must be cyclical, not linear. “Fix and forget” is not a viable long term risk management strategy due to the dynamic and rapid evolution of business and technology. The feed-back loop from monitoring to re-assessment helps to ensure the risk management program remains dynamic and in step with organizational goals and operations.

Control Environment Observations

At the system level, we found similar opportunities for improvement across all systems. Our analysis of this consistency is that system-level weaknesses are merely symptomatic of enterprise-level issues. Improvements to risk management processes at the enterprise level are likely to result in long-term benefits at the systems level. This is not to imply that improvements cannot and should not be made at the system level—they can and we recommend they should be made. Without enterprise-level risk management support, guidance, and monitoring, system-level problems will tend to reoccur.

We used GAO’s Risk Management Cycle as the basis for measuring compliance with federal privacy and security guidance. We related the control areas from a NIST-compliant security plan to each of the four stages in GAO’s risk management cycle, a process called “binning.” A-130 Appendix I, A-130 Appendix III and security guidance contained in NIST Special Pub 800-14 and Special Pub 800-18 provided the specific standards against which we could measure SFA system compliance.

We first attempted to assess compliance vertically, examining the level of compliance for each system in each issue/control area, taking into account the business process supported by each system. A “stop light” grade was assigned to each issue/control area. One of the challenges that had to be addressed was the failure of several systems to respond in timely fashion to the survey team requests for information. Rather than leave blanks where current information was not made available, we used information contained in previous risk assessments and control reviews from the past three years. In many cases several such reports were available for individual systems. In order to make clear what is current information and what is not, information taken from recent surveys is highlighted as red text in the system-specific tables. In some instances, no information—past or current—on certain controls for certain systems was available. In these cases we were forced to assume total non-compliance.

Using this method, ‘red’ indicates either total non-compliance or serious shortcomings; ‘yellow’ indicates either less than full compliance or room for improvement, and ‘green’ indicates either sufficient or full compliance although it does not mean there is no room for additional improvement. Grades were assigned subjectively; generally, any failure to fully measure up to the articulated standard was sufficient for a ‘yellow’ grade, while lack of evidence for compliance, or evidence of numerous shortcomings resulted in a ‘red’ grade.

In this task a vulnerability was considered to be anything that fell short of Federal guidance. However, we also looked beyond compliance to consider what other measures might be taken to improve enterprise and system level risk management. *For this reason there are a number of instances where opportunities for*

improvement are provided at the enterprise and system levels for control areas that have been given a green stoplight.

Once grades were assigned at the system level, we then evaluated compliance horizontally, examining the consistency of compliance across all systems for each issue/control area. This horizontal view enabled us to assess the overall effectiveness and consistency of privacy and security controls at SFA. For this arena we assigned grades based on the lowest three system level grades; if six of nine systems were 'green,' but three were 'yellow,' the overall grade assigned to that control area was yellow. Both enterprise-wide and system-specific stoplight charts are included in this report; the enterprise-wide view is available beginning with the illustration of the [GAO Risk Management Cycle](#) below; system-level charts are accessible from this section via hot links.

In summary, the goal of this document is to allow SFA managers to take in at a glance the overall maturity of their risk management process, to understand their current level of compliance with OMB guidance, and to provide useful, cost-effective recommendations for improving risk management processes.

Overview of SFA System Risk Management Maturity

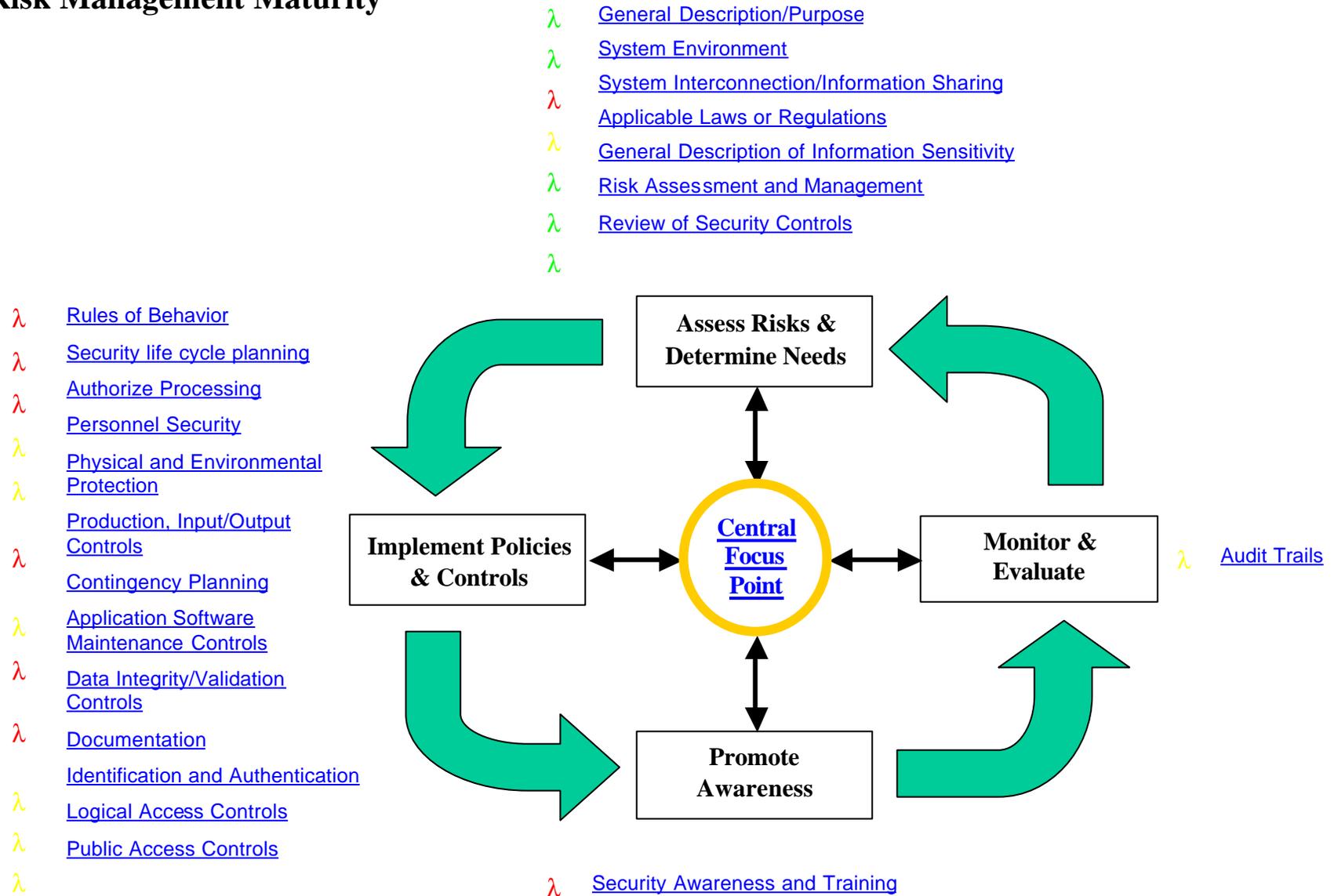


Figure 1: SFA System Risk Management Maturity Overview

Central Security Focus/Assigned Security Responsibility

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

Standard: [OMB A-130](#), [NIST Special Pub 800-14](#)

1 [DLCD/DLSS](#)

A *central security program*... should have the following:

1 [DLOS](#)

- Stable Program Management Function
- Existence of Policy
- Published Mission and Functions Statement.
- Long-Term Computer Security Strategies
- Compliance Program
- Intraorganizational Liaison
- Liaison with External Groups

1 [FFEL](#)

1 [NSLDS](#)

By definition, major applications are high-risk and require special management attention. It is important, therefore, that an individual be assigned responsibility in writing to assure the particular application has adequate security. To be effective, this individual should be knowledgeable in the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect the application.

1 [RFMS](#)

1 [PEPS](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

1 [TIVWAN](#)

None of the security program functions noted above can be effective if SFA management lacks the knowledge basis to fulfill their responsibility of overseeing the risk management processes. Most managers and security officers do not have security backgrounds; in the near term only training can provide them with the needed knowledge baseline.

Current Status:

- Intraorganizational Liaison
- Liaison with External Groups

Program management functions appear to be typical of those found in other government agencies of similar size and complexity to SFA, albeit most system management functions have been outsourced to the various system vendors.

Policies—particularly those relating to information security and personnel management—exist at the ED level and are adequate for their purposes. However, available evidence indicates SFA system-level awareness of those policies is not consistent and is non-existent in some cases.

As noted below in [General Description/Purpose](#), descriptions of system mission and functions statements could be much improved even though in the strictest sense they are adequate for compliance purposes.

Interviews with systems personnel indicate a number of systems are in evolutionary acquisition, and SFA is planning the merger of disparate systems under a single architecture similar to the EDCAPS initiative at ED. However, despite the evidence in interviews and informal conversation, no formal documentation was in evidence.

In reviewing the survey responses, we found the maturity of compliance programs varied from system to system. For example, DLOS reports reviewing security logs on a weekly basis, while NSLDS does not collect audit data at all, relying only on the access logs recorded by RACF—an inadequate basis for a robust compliance program.

In the current paradigm the vendors provide security over their own systems – many are under the same roof at the Meriden VDC and benefit from security controls over that facility – however, if it exists, liaison between systems for security purposes appears to take place only on an informal basis and there was no evidence at all of regular interface with external organizations other than vendors and auditors.

While the System Security Officers (SSOs) of the surveyed systems generally appear to be knowledgeable of the information and process supported by their respective applications, they do not appear to be conversant with the management, personnel, operational, and technical controls used to protect their respective application. While a number are new to their positions, all appear to rely heavily on contractors to administer the security function. Security, in effect, has been outsourced.

Guidelines, formal system security documentation and strategies, a compliance program, intra- and extra-organizational liaison were not evident (see the discussion of [documentation](#)).

While this situation is not in itself untenable, the lack of qualified oversight increases the risk to government interests. SSOs must have a minimum level of training and authority in order to serve the central coordination function that is required to initiate and perpetuate the risk management cycle. Contractors, regardless of how well intentioned or contractually bound, cannot be viewed as competent to provide security oversight on a system their company developed; doing so invariably creates a security environment in which conflict of interest is built-in.

The general lack of security program structure at the system level is symptomatic of this lack of focus and training. Generally, while evidence of many security program features could be found within individual systems, the security structure across the board is weak, with many of the required pieces of a mature security program (formal system-level policies, standards, and procedures) missing.

Opportunities for Improvement:

Most of the security program shortcomings noted above are discussed in greater detail in the body of this document below, so they will not be covered here. However, it is important to note that no security program can be effective when the staff responsible for its oversight is not qualified; all of the central security program features listed above cannot be effective without a knowledgeable security staff. SFA should therefore ensure security officers possess skills commensurate with their responsibilities. Going forward, the qualification and training process for SSOs should be more rigorous; only those who have security experience and training should be assigned, and SFA should give preference to those who have earned formal certifications [e.g., Certified Information Systems Auditor (CISA) or Certified Information System Security Professional (CISSP)], or who have some other formal security qualification. In the near term, current SSOs should be provided with training in security theory and practice. SFA should first look to GSA training offerings, and if suitable government training opportunities are not found (or do not prove cost-effective), training by commercial provider should be considered.

1 [CBS](#)

General Description/Purpose

1 [CPS](#)

[Back to Risk Cycle Illustration](#)

1 [DLCD/DLSS](#)

STANDARD: [NIST SPECIAL PUB 800-18](#)

Present a brief description (one-three paragraphs) of the function and purpose of the system (e.g., economic indicator, network support for an organization, business census data analysis, and crop reporting support).

1 [DLOS](#)

If the system is a general support system list all applications supported by the general support system. Specify if the application is or is not a major application and include unique name/identifiers, where applicable. Describe each application's function and the information processed. Include a list of user organizations, whether they are internal or external to the system owner's organization, and a general description of the type of information and processing provided. Request information from the application owners (and a copy of the security plans for major applications) to ensure their requirements are met.

1 [FFEL](#)

1 [NSLDS](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

1 [RFMS](#)

Accurate, complete system descriptions in system security plans provide several long term benefits.

1 [PEPS](#)

System descriptions are required in many federal documents – A-130 reviews, security audits, certification and accreditation documents, etc. By providing a full, complete, and accurate system description in the system security plan, all other documents requiring this information can draw from a single source. This reduces the potential for conflicting information across several reports, helps to reduce the risk that out-of-date information is carried forward into future documentation, reduces the amount of time spent in duplicative information-gathering efforts, and provides managers and security staff with a single, authoritative source of information.

1 TIVWAN

Current Status:

While all systems were described to one level of detail or another, and strictly speaking meet the criteria for compliance, the description content was inconsistent and where multiple descriptions for a single system were found they often conflicted with one another.

Few network diagrams exist. The diagrams that were obtained had not been dated and some had limited utility because they portray business process rather than technical architecture, even when used to support a technical document. Further, no accurate description of one system's technical architecture was found at all.

The amount of time required by KPMG, SFA, and system contractor staff to gather this data illustrates the value of maintaining complete, accurate, and up-to-date descriptions.

Opportunities for Improvement:

Ensure consistent, complete and accurate descriptions, including detailed network and business process diagrams, are included in system security plans. Descriptions should be thoroughly vetted prior to publication. Once complete, all descriptions and diagrams should be prominently dated and signed by the SSO and forwarded to the OCIO Champion for Privacy and Security for information. Subsequently any document that calls for a system description should draw on this source. The SSO should re-validate the process every six months, or after a major system move/modification, whichever comes first.

1 [CBS](#)

System Environment

1 [CPS](#)

[Back to Risk Cycle Illustration](#)

Standard: [NIST Special Pub 800-18](#)

1 [DLCD/DLSS](#)

Provide a general description of the technical system. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.)

1 [DLOS](#)

Describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources.

1 [FFEL](#)

Include any security software protecting the system and information.

1 [NSLDS](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

Remarks made in the [General Description](#) section apply here as well.

1 [RFMS](#)

Current Status:

While information exists to allow many systems to be rated as in compliance, in most cases the descriptions of systems environment are just barely adequate, and few network diagrams exist. The diagrams that were obtained had not been dated and some had limited utility because they portray business process rather than technical architecture, even when used to support a technical document. Further, no accurate description of one system's technical architecture was found at all.

1 [TIVWAN](#)

Opportunities for Improvement:

Barely adequate documentation can be greatly improved with minimal effort. Remarks made in the [General Description](#) section apply here.

System Interconnection/Information Sharing

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

Standard: [NIST Special Pub 800-18](#)

1 [DLCD/DLSS](#)

OMB Circular A-130 requires that written management authorization (often in the form of a Memorandum of Understanding or Agreement,) be obtained prior to connecting with other systems and/or sharing sensitive data/information.... It is required that written authorization (MOUs, MOAs) be obtained prior to connection with other systems and/or sharing sensitive data/information. It should detail the rules of behavior that must be maintained by the interconnecting systems. A description of these rules must be included with the security plan or discussed in this section.

1 [DLOS](#)

1 [FFEL](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

Formal Memorandums of Understanding (MOUs) or Memorandums of Agreement (MOAs) that define service levels and standards of behavior increase management's confidence that information security and privacy policies and standards are being followed in areas outside SFA's normal control responsibility. If a system's boundaries can be defined by the business process it supports, then many SFA *system* boundaries are outside SFA's *control* boundary (e.g., on institution campuses). Formal chain-of-trust agreements with these external agencies help to extend SFA management's control boundary closer to system boundaries. While implementing compliance monitoring mechanisms may prove difficult or impractical, SFA management may at least have the confidence that proceeds from an agreed-upon set of technical and privacy/security standards.

1 [NSLDS](#)

1 [RFMS](#)

1 [PEPS](#)

Current Status:

While rules of behavior and system interfaces are described in varying detail, no MOUs or MOAs were identified.

1 TIVWAN

Opportunities for Improvement:

Develop a standard MOA to describe technical interfaces with information sharing partners. The MOA template should call for:

- A description of the control boundary between SFA and external organization (i.e., the last router/hub/switch/ firewall under SFA control, along with the physical location of the device or devices).
- A description of the interface at each layer of the applicable protocol stack (e.g., SNA model: physical, data link, path control, transmission control, data flow control, presentation services, transaction services; OSI model: physical, data link, network, transport, session, presentation, application).

Develop a separate MOU to define security and privacy expectations. Reference applicable laws, regulations, and policies; define agree-upon standards, procedures and guidelines as appropriate.

Applicable Laws and Regulations

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

1 [DLCD/DLSS](#)

1 [DLOS](#)

1 [FFEL](#)

1 [NSLDS](#)

1 [RFMS](#)

1 [PEPS](#)

1 [TIVWAN](#)

Standard: [NIST Special Pub 800-18](#), [Privacy Act of 1974](#), [OMB A-130 Appendix I](#)

List any laws, regulations, or policies that establish specific requirements for **confidentiality, integrity, or availability** of data/information in the system.

Comply with the provisions of the Privacy Act, Appendix I of A-130

SIGNIFICANCE IN THE SFA ENVIRONMENT:

The Office of Student Financial Assistance (SFA) collects and maintains sensitive Privacy Act data, including name, address, social security number, birthdate, as well as financial information, including income and assets, and tax information, relating to a student loan applicant and the applicant's family. It is unlawful to collect, use, or disclose privacy data except in accordance with the authorized uses for which the data was collected. Unauthorized disclosures or compromise of privacy act data could result in severe adverse consequences to the applicant, and adverse public reaction and/or liability for the agency that improperly collected, used, or disclosed the data.

Current Status:

Lists of applicable laws at varying levels of detail exist for all systems; in this regard all systems are compliant.

However, Privacy Act compliance was less easy to measure as privacy questionnaires were for the most part not returned, resulting in the yellow stoplights displayed at left. However, we did determine there are currently eight published notices for systems of records within the SFA Assistance. Those notices appear to be current. Information about privacy act data is provided by each system manager to SFA's analysis staff, which prepares draft notices. Draft notices are reviewed by the Department of Education's Office of General Counsel. Responsibility for publication of these notices, as well as annual or biennial review of systems of records notices, routine use disclosures associated with each system of records, exemptions, and matching programs, seems to lie with the Department of Education's Privacy Officer.

OPPORTUNITIES FOR IMPROVEMENT:

Employees and contractors are cognizant of the need to protect Privacy Act data, and are familiar with which data is protected. Awareness of the exact number of systems of records, where the systems are located, and many of the pertinent specific requirements of the Privacy Act, such as logging disclosures and providing individuals with access to their own data is more limited. Improved training on the specific requirements of the Privacy Act would help to increase awareness and ensure compliance (see recommendations under [Security Training and Awareness](#)).

Description of Information Sensitivity

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

Standard: [NIST Special Pub 800-18](#)

1 [DLCD/DLSS](#)

Describe, in general terms, the information handled by the system and the need for protective measures. Relate the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability). For each of the three categories, indicate if the requirement is: **High, Medium, or Low**.

1 [DLOS](#)

Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.

1 [FFEL](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

1 [NSLDS](#)

A security model that categorizes information sensitivity and assigns information ownership is a keystone activity in establishing a control environment. SFA systems process, store and transmit a great deal of sensitive information, including information protected by the Privacy Act and other financial information that must have its integrity maintained. Safeguarding the privacy and security of sensitive information requires all managers, system operators, and users to proceed from a common understanding of varying levels of information sensitivity, as well as the protection standards that apply to each.

1 [RFMS](#)

Current Status:

1 [PEPS](#)

Systems that have recent A-130 reviews have had information sensitivity and magnitude of harm defined, and annual Privacy Act training is reported to take place. However, information sensitivity descriptions are defined in very general terms; existing descriptions provide no specific information concerning information inputs and outputs by interface, method of input (e.g., keyboard entry, batch process) or output (e.g., print job, web publishing), and the specific nature of the information in question. In addition, information sensitivity is not defined and not evident for a number of systems.

1 [TIVWAN](#)

Opportunities for Improvement:

Here again is an instance where SFA could benefit from going beyond mere compliance with the NIST standard; more detailed descriptions of information sensitivity and the handling requirements for each category would provide benefits during system audit, system certifications, and risk assessments.

Each system should have all information inputs and outputs defined. Just as with system environment descriptions, system management should ensure complete and accurate descriptions of the information that is processed, stored, and transmitted by their respective systems is documented. These descriptions should describe the overall information flow in, through, and out of the system from a business process perspective, discrete information types by sensitivity level, laws and regulations as they apply to each type of information, and the consequences of compromise to information privacy, security, integrity, and availability. Of note, much of this information may be easily derived from Y2K documentation; while Y2K documents tend to view risk from a hardware or software perspective, information availability consequences may be inferred. Descriptions should be thoroughly reviewed prior to publication. Once complete, all descriptions should be prominently dated and signed by the SSO and forwarded to the OCIO Champion for Privacy and Security for information. Subsequently, any document that calls for a system description should draw on this source. The SSO should re-validate process every six months, or after a major system move/modification, whichever comes first.

Risk Assessment and Management

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

Standard: [OMB A130](#)

1 [DLCD/DLSS](#)

While formal risk analyses need not be performed, the need to determine adequate security will require that a risk-based approach be used. This risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.

1 [DLOS](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

1 [FFEL](#)

Risk assessment is another keystone activity in the GAO risk management cycle. The goal of risk management is to establish an effective and cost-beneficial control environment in which information is protected in a manner commensurate with its sensitivity and value. Risk assessment should provide a baseline understanding of vulnerabilities, threats, and relative risk; this in turn may serve as a reasonable basis for making management decisions on what controls and risk mitigation measures are appropriate in a given systems environment. Without this baseline systems managers cannot make *deliberate* risk decisions. In consequence, resources may not be efficiently allocated; managers may spend too much (or too little) time, effort and expense mitigating risks. Over-compensating for risk does not make good business sense, particularly in the resource-constrained government environment. But neither can a business case be made for under-compensating for risk; a single incident can easily wipe out whatever might have been 'saved' by not employing the proper risk mitigation measure. In addition, SFA managers have a public-service obligation to take measures to maintain public confidence in government. Privacy and security breaches may undermine this confidence; this as much as anything else recommends SFA take a purposeful approach to risk management.

1 [NSLDS](#)

1 [RFMS](#)

1 [PEPS](#)

Current Status:

1 [TIVWAN](#)

This risk assessment serves to allow a green stoplight for all surveyed systems, however, some of information uncovered in the course of this assessment is of concern. For example, three of the nine systems surveyed had not undergone a risk assessment in the last three years, and while six systems had, it is not clear from the available evidence that the results of these risk or controls assessments feed into a structured risk management program.

Opportunities for Improvement:

Generally, SFA should strive to implement and put into motion the risk management cycle recommended by GAO. This cycle should be applied at the individual systems level, with proactive oversight provided from the OCIO level. For further analysis and detailed recommendations, refer to the [Discussion](#), [Conclusions](#), and [Recommendations](#) sections of this document.

Review of Security Controls

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

Standard: [OMB A-130](#)

1 [DLCD/DLSS](#)

At least every three years, an independent review or audit of the security controls for each major application should be performed. Because of the higher risk involved in major applications, the review or audit should be independent of the manager responsible for the application. Such reviews should verify that responsibility for the security of the application has been assigned, that a viable security plan for the application is in place, and that a manager has authorized the processing of the application.

1 [DLOS](#)

1 [FFEL](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

Risk assessment and controls reviews are very closely related; both are crucial activities in the risk management cycle. While risk assessment is technically the process through which management determines what undesirable things could happen, and controls reviews are designed to assess the effectiveness of risk mitigation measures, in practice, both risk and controls are often addressed together in such reports as A-130 compliance reviews.

1 [NSLDS](#)

1 [RFMS](#)

As discussed above in [Risk Assessment and Management](#), SFA managers should concern themselves with ensuring controls are in place and operating to deliberately and effectively manage risk to sensitive information. Doing so not only makes good business sense, but also helps SFA satisfy its public-service obligations.

1 [PEPS](#)

Current Status:

1 [TIVWAN](#)

Again, this survey allows a green spotlight for all surveyed systems, however, some of information uncovered in the course of this assessment is of concern. Controls assessments of one variety or another have been conducted within the last three years on six of the nine systems surveyed for this report. Altogether these reports document 193 separate findings, but it is not clear from the obtained evidence exactly how many have been addressed or resolved. Current efforts appear to center on addressing each individual finding, however, there is little available evidence that points to an enterprise-level effort to examine and address the organizational or systemic shortcomings that allow these weaknesses to develop. In other words only the symptoms, not the root causes, are being addressed.

Opportunities for Improvement:

Future controls assessments should be used to measure the maturity of SFA's [risk management cycle](#). This will better empower SFA managers to tackle the fundamental conditions that result in risk rather than focus on the symptomatic manifestations of those conditions. For further analysis and detailed recommendations, refer to the [Discussion](#), [Conclusions](#), and [Recommendations](#) sections of this document.

1 [CBS](#)

Rules Of Behavior

1 [CPS](#)

[Back to Risk Cycle Illustration](#)

Standard: [OMB A130](#)

1 [DLCD/DLSS](#)

Rules of behavior should be established which delineate the responsibilities and expected behavior of all individuals with access to the application. The rules should state the consequences of inconsistent behavior. Often the rules will be associated with technical controls implemented in the application. Such rules should include, for example, limitations on changing data, searching databases, or divulging information.

1 [DLOS](#)

1 [FFEL](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

Rules of behavior that define expected and prohibited behavior increase management's confidence that information security and privacy policies and standards are being followed by the system users. Users cannot reasonably be expected to remember in detail the laws, regulations, policies, standards, procedures and guidelines that govern the operation and use of a system. However, well-defined rules of behavior can distill the intent of law and policy into a form that is easily grasped and retained. In addition, while policies and standards are intended more to provide guidance to decision-makers, rules of behavior are designed to provide day-to-day guidance to users. Combined with a robust privacy and [security awareness and training](#) program, system rules of behavior help to ensure that everyone granted authorized access to SFA systems behaves in a consistently secure and ethical fashion.

1 [NSLDS](#)

1 [RFMS](#)

Current Status:

Rules of behavior have not been articulated for seven out of nine systems.

1 [PEPS](#)

1 [TIVWAN](#)

Opportunities for Improvement:

Where practical, develop rules of behavior that are identical for all systems. As required, augment these common rules with additional guidance specific to each system. NSLDS and PEPS rules of behavior provide examples of what may be considered acceptable.

1 [CBS](#)

Security Life Cycle Planning

[Back to Risk Cycle Illustration](#)

1 [CPS](#)

Standard: NIST Special Pub 800-14, [NIST Special Pub 800-18](#)

1 [DLCD/DLSS](#)

Security, like other aspects of an IT system, is best managed if planned for *throughout* the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal....

1 [DLOS](#)

Organizations should ensure that security activities are accomplished during each of the phases....

1 [FFEL](#)

Initiation Phase: Document the need and purpose for the system. Perform an information sensitivity assessment.

Development/Acquisition Phase: Develop security requirements at the same time system planners define the requirements of the system.

1 [NSLDS](#)

Implementation Phase: Configure and enable the system's security features; test, install, field, authorize for processing.

Operation/Maintenance Phase: Describe the security activities conducted or planned as the system evolves. The security plan documents the security activities.

1 [RFMS](#)

Disposal Phase: Briefly describe in this section how information is disposed of and how media are sanitized.

1 [PEPS](#)

I TIVWAN

Significance in the SFA Environment:

Information and the technology that supports it represent SFA's most valuable assets. Moreover, SFA's customer base—students and educational institutions—have heightened expectations regarding service delivery. For this reason SFA customers require increased quality, functionality, and ease of use, decreased loan processing time, and continuously improving service levels. The constrained resource environment within the Federal government requires all these goals to be accomplished at lower cost and reduced risk. Success, however, requires SFA managers to understand and manage the risks associated with implementing and operating technologies that handle sensitive information.

One of the keys to success requires privacy, security, and risk management principles to be knit into the systems life cycle. Security controls are always more expensive to retrofit than to design-in; accordingly, privacy and security should be considered in the very earliest stages of systems development and follow through the life cycle to disposal. Similarly, information passes through a predictable life cycle; controls must be in place at every stage in that life cycle from creation or entry through disposal. Planning for privacy and security in the life cycle will help SFA optimize its information investment, and mitigate information and business process risks when things go wrong.

Current Status:

Beyond the most rudimentary controls, there was little evidence to suggest that privacy and security considerations play a role in system life cycle planning; security in particular does not appear to be well-integrated into the system life cycle process. In addition, we found little awareness of existing ED system life cycle policies and guidance.

Opportunities for Improvement:

SFA system managers should ensure the information security life cycle is addressed in system life cycle planning documents; security controls and risk mitigation measures should be described for every stage in the information life cycle as they apply to the stages of the system life cycle. Discuss at minimum information risk controls for the following stages:

- Collection/Creation
- Processing (i.e., integrity and validation controls at data entry, conversion and/or manipulation)
- Storage
- Transmission
- Application (i.e., controls between processes, systems, or applications)
- Disposal

Authorize Processing

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

Standard: [OMB A-130](#)

1 [DLCD/DLSS](#)

Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented secures the application adequately. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter.

1 [DLOS](#)

Management authorization implies accepting the risk of each system used by the application.

1 [FFEL](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

Risk management is a necessary activity in any systems environment because risk is a fact of life in virtually all IT environments – there is no such thing as a risk-free system. In consequence, before an SFA system becomes operational it makes sense for senior SFA management to decide how much risk must be mitigated prior to system use, or conversely, how much residual risk can be accepted. This is the purpose of the certification and accreditation process; to decide whether risk is mitigated to the point where from a business and legal perspective it is safe to allow a system to process information. In order to provide SFA managers with a reasonable basis for accreditation – risk acceptance – some sort of technical review must be conducted to determine if the systems' automated and procedural controls are sufficient to enforce SFA security policies and standards. In this way, risk decisions can be made deliberately rather than by default.

1 [NSLDS](#)

1 [RFMS](#)

1 [PEPS](#)

Current Status:

Available evidence indicates that only the Pell system has undergone a formal certification and accreditation process. Several other systems have been authorized to operate on the basis of an A-130 review, but we found no evidence of formal certification processes. In addition, many systems have not had processing re-authorized every three years.

I TIVWAN

Opportunities for Improvement:

At OCIO discretion, grant all systems an interim authority to operate (IATO) for one year. Within eighteen months from issuance of the IATO, each system should perform a formal certification test under the guidance provided in FIPS 102, *Guideline for Computer Security Certification and Accreditation*, and be accredited by cognizant ED/SFA authority. Serious shortcomings identified in the testing process should be fully addressed prior to final accreditation.

Personnel Security

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

Standard: [OMB A-130](#)

1 [DLCD/DLSS](#)

For most major applications, management controls such as individual accountability requirements, separation of duties enforced by access controls, or limitations on the processing privileges of individuals, are generally more cost-effective personnel security controls than background screening. Such controls should be implemented as both technical controls and as application rules. For example, technical controls to ensure individual accountability, such as looking for patterns of user behavior, are most effective if users are aware there is such a technical control. If adequate audit or access controls (through both technical and non-technical methods) cannot be established, then it may be cost-effective to screen personnel, commensurate with the risk and magnitude of harm they could cause. The change in emphasis on screening in the Appendix should not affect background screening deemed necessary because of other duties an individual may perform

1 [DLOS](#)

1 [FFEL](#)

1 [NSLDS](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

SFA is responsible for disbursing millions of dollars annually in student aid. In this process, SFA must accurately account for allocated funds, reconcile accounts, handle personal information on thousands of individuals, and interact with hundreds of government, private, and commercial institutions. In recognition of the sensitivity of this mission and the systems, information, and processes that support that mission, the Department of Education has articulated policies and procedures for identifying sensitive positions. These policies and procedures are outlined in ED's *Personnel Security Suitability Program Handbook*. Dated November 4, 1992, and issued by the ED Office of the Inspector General (OIG), this handbook was issued to implement 5 CFR Parts 731, 732, 736 and 754, and outlines ED's personnel security suitability policies, procedures, and guidelines.

1 [RFMS](#)

1 [PEPS](#)

1 [TIVWAN](#)

Current Status:

ED guidance with regard to defining sensitive positions and reviewing personnel in sensitive positions is not being applied consistently across all systems, as evidenced by SFA staff and vendor system managers' lack of knowledge that such guidance exists.

Opportunities for Improvement:

With OCIO oversight, implement ED personnel security guidance consistently across all systems. Ensure that:

- Sensitive Positions are identified and classified
- All government personnel in sensitive positions have been properly investigated and designated in writing by the OCIO and/or system Functional Managers
- All personnel in sensitive positions receive security awareness training commensurate with their position and responsibility.

Physical and Environmental Protection

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

Standard: [NIST Special Pub 800-18](#)

1 [DLCD/DLSS](#)

An organization's physical and environmental security program should address the following seven topics:

1 [DLOS](#)

- Physical access controls
- Fire safety factors
- Failure of supporting utilities
- Structural collapse
- Plumbing leaks
- Interception of data
- Mobile and portable systems

1 [FFEL](#)

1 [NSLDS](#)

1 [RFMS](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

Physical and environment protections are especially important, given the recent systems consolidation into the [Meriden VDC](#). A single incident stemming from a physical security breach or environmental problem could impact the operations for seven out of the nine systems surveyed.

1 [PEPS](#)

Current Status:

1 [TIVWAN](#)

We could find no description of physical and environmental controls for the PEPS system, and the previous security or controls-related surveys indicate flaws in physical controls. While none are particularly serious, weaknesses in the [contingency planning](#) process heightens the concern for this control area.

Opportunities for Improvement:

When developing/updating system security plans, ensure the controls noted above are fully addressed. In addition, CSC should be requested to ensure all of the above noted controls are addressed in future SAS-70 reports for the Meriden VDC.

Production, Input/Output Controls

[Back to Risk Cycle Illustration](#)

I [CBS](#)

I [CPS](#)

I [DLCD/DLSS](#)

I [DLOS](#)

I [FFEL](#)

I [NSLDS](#)

I [RFMS](#)

I [PEPS](#)

I [TIVWAN](#)

STANDARD: [NIST SPECIAL PUB 800-18](#)

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to, application software should be listed. In this section, provide a synopsis of the procedures in place that support the operations of the application.

SIGNIFICANCE IN THE SFA ENVIRONMENT:

Input and output controls are a part of [security life cycle planning](#). SFA systems are complex and, even in the context of the [Meriden VDC](#), are located and operated in a diverse and complex environment. In these circumstances, sensitive information (and the applications that process, store, and transmit it) are vulnerable to compromise and corruption. As noted in Special Pub 800-18, "...appropriate and adequate controls will vary depending on the individual system requirements..."; the accreditation authority, in coordination with system management and security authorities, should determine what controls are appropriate. At a minimum, applications that handle sensitive information should have controls for marking, handling, processing, storage, and disposal that are sufficient to ensure this information is not mishandled through error.

Current Status:

It was difficult to assess the status of input/output controls for six of the nine systems surveyed because there was little evidence available. While production and input/output controls almost certainly exist, they are not documented. Inquiries concerning them were not answered. In many cases the only evidence available was through past system-specific security reviews that indicated opportunities for improvement are numerous.

Opportunities for Improvement:

Regarding opportunities for improvement, see the opportunities for improvement section for [security life cycle planning](#). Controls for monitoring application software installation and update should be governed by the [system certification and accreditation](#) and [application software maintenance control](#) processes.

Contingency Planning

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

1 [DLCD/DLSS](#)

STANDARD: [OMB A-130](#)

Managers should plan for how they will perform their mission and/or recover from the loss of existing application support, whether the loss is due to the inability of the application to function or a general support system failure. Experience has demonstrated that testing a contingency plan significantly improves its viability. Indeed, untested plans or plans not tested for a long period of time may create a false sense of ability to recover in a timely manner.

1 [DLDS](#)

1 [FFEL](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

SFA has made a business decision to consolidate many of its systems' servers in CSC's [Meriden VDC](#). While this helps to achieve economies of scale, it also increases SFA's vulnerability to the threat of a single, catastrophic failure at the VDC. In addition, if SFA's go-forward strategy integrates several systems into one, similar to the EDCAPS integration, further economies and efficiencies may be realized. However, the more the SFA business process relies on a single system, the greater the risk resulting from the loss of the system and/or compromise of the information it processes.

1 [NSLDS](#)

1 [RFMS](#)

Current Status:

Available evidence indicates that both contingency planning and incident response plans and processes are immature. In some cases there is no evidence that plans and procedures exist. In cases where they exist there is no evidence they have been tested to ensure they will work. Further evidence indicates many SSOs are unfamiliar with contingency procedures, and in many cases have not even had access to contingency and incident response plans and procedures.

1 [PEPS](#)

1 [TIVWAN](#)

OPPORTUNITIES FOR IMPROVEMENT:

Ensure that CSC and other cognizant vendors have formal contingency and incident response plans, that these incident response plans are consistent with guidance contained in NIST Special Pub 800-3, *Establishing a Computer Security Incident Response Capability (CSIRC)*, and that cognizant SSOs have copies of these plans. Ensure that within the next year all contingency and incident response plans have been tested.

Application Software Maintenance Controls

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

1 [DLCD/DLSS](#)

1 [DLOS](#)

1 [FFEL](#)

1 [NSLDS](#)

1 [RFMS](#)

1 [PEPS](#)

Standard: [NIST Special Pub 800-18](#)

Application controls should be established to monitor the installation and updates to application software to ensure software functions as expected and that a historical record is maintained of application changes.

SIGNIFICANCE IN THE SFA ENVIRONMENT:

As noted elsewhere in this report, the collective SFA systems environment is moderately large in terms of size, scale, complexity, and interconnectivity. Many systems and applications are required to support the SFA business process; these are developed, operated and maintained by multiple software developers. If software maintenance controls are not in place or operating effectively, unauthorized or unintended changes to application software can result in privacy or security compromises to information in the system, which may impact SFA's ability to properly service its customers. In addition, due to the interconnectedness of SFA and ED systems, errors in one application may propagate to other applications in the system in question.

Current Status:

Available evidence indicates that system development environments and configuration management (CM) procedures vary widely. In some cases, documented practices introduce significant risk and run contrary to generally accepted best practices (e.g., test and development environments not separated, security personnel not involved in the CM process).

1 TIVWAN

Opportunities for Improvement:

Examine ED guidance relating to system life cycle planning, and ensure that:

- CM processes and procedures are consistent across all systems. System development contractors should be presented with a minimum set of development and CM standards; compliance with these standards should be incorporated into service-level agreements as soon as possible.
- SSOs are integrated into the systems development and CM processes. SSOs should be part of the approval chain for all proposed changes to system software to avoid changes being made that would compromise privacy or security controls, and to enable the SSOs to act as the accrediting authority's agent in between certification cycles.

Data Integrity/Validation Controls

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

STANDARD: [NIST SPECIAL PUB 800-18](#)

1 [DLCD/DLSS](#)

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirement. Describe any controls that provide assurance to users that the information has not been altered and the system functions as expected.

1 [DLOS](#)

Data integrity controls include antivirus software, reconciliation routines, edit checks, intrusion detection, message authentication codes, and system performance monitoring.

1 [FFEL](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

1 [NSLDS](#)

Information enters SFA systems by multiple sources, some within SFA's span of control but many not. Integrity and validation checks help to ensure that as information enters, is processed, and is output from the system, it retains its integrity. As noted above for [application software maintenance controls](#), the interconnected nature of SFA systems make continued data integrity a crucial issue; information corruption can propagate throughout the system, impacting SFA's efficient execution of its business processes.

1 [RFMS](#)

Current Status:

1 [PEPS](#)

Available evidence suggests that integrity and validation controls receive little if any attention in survey systems' environments.

1 [TIVWAN](#)

Opportunities for Improvement:

Establish standards for data integrity and automated validations. Such standards may address limit, range, and syntax checking for data fields, checksums and hash totals, automated reconciliation routines, etc. Develop a plan for implementing/upgrading edit and validation mechanisms as part of each system's individual lifecycle/upgrade plans. Identify inter-system edit and validation opportunities; OCIO provides coordination between system owners to implement identified control opportunities.

Documentation

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

Standard: OMB A-130, [NIST Special Pub 800-18](#)

1 [DLCD/DLSS](#)

Plan for adequate security of each general support system as part of the organization's information resources management (IRM) planning process. The security plan shall be consistent with guidance issued by the National Institute of Standards and Technology (NIST)...Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST...

1 [DLOS](#)

Documentation should be coordinated with the general support system and/or network manager(s) to ensure that adequate application and installation documentation are maintained to provide continuity of operations....

1 [FFEL](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

1 [NSLDS](#)

System documentation (e.g., system description, technical interface description, system manager manual, user manual, security policy and standards, security features users guide, risk assessment, certification test reports, operational procedures and guidelines, etc.) help to establish a common baseline of knowledge for managers, developers, operators and users. This baseline is especially important in a complex, interconnected multi-system environment such as SFA's. In the SFA environment it is common for managers, staff, contractors, and non-SFA government employees to require information concerning SFA systems. Well maintained documentation ensures, for example, that other system developers who are writing code to interface with an SFA system have authoritative interface documentation to draw from. Similarly, as noted in the [systems environment](#) section above, adequate documentation promotes increased efficiency and effectiveness across a wide range of activities.

1 [RFMS](#)

1 [PEPS](#)

1 [TIVWAN](#)

CURRENT STATUS:

Overall, system and security documentation is very inadequate. System descriptions, technical descriptions and illustrations, security plans and procedures are either not in evidence, inadequate, or do not fully satisfy the guidance and intent of [NIST Special Pub 800-18](#).

Opportunities for Improvement:

Develop NIST-compliant security plans for all SFA systems. Take action on the opportunities for improvement articulated in [general description](#) and [systems environment](#) sections.

1 [CBS](#)

1 [CPS](#)

1 [DLCD/DLSS](#)

1 [DLOS](#)

1 [FFEL](#)

1 [NSLDS](#)

1 [RFMS](#)

1 [PEPS](#)

1 [TIVWAN](#)

Identification and Authentication

[Back to Risk Cycle Illustration](#)

STANDARD: [NIST SPECIAL PUB 800-14](#), [NIST SPECIAL PUB 800-18](#)

Identification and authentication (I&A) is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability.

- Describe the major application's authentication control mechanisms.
- Describe the method of user authentication (password, token, and biometrics).
- Provide the following if an additional password system is used in the application:
 - password length (minimum, maximum)
 - allowable character set,
 - password aging time frames and enforcement approach,
 - number of generations of expired passwords disallowed for use
 - procedures for password changes (after expiration and forgotten/lost)
 - procedures for handling password compromise
- Indicate the standards for of password changes.
- Describe how the access control mechanism supports individual accountability and audit trails.
- Describe the standards for password syntax.
- Describe the standards for password protection.
- State the number of invalid access attempts that may occur and describe the actions taken when that limit is exceeded.
- Describe the procedures for verify ing that all system-provided administrative default passwords have been changed.
- Describe the procedures for limiting access scripts with embedded passwords.
- Describe any policies that provide for bypassing user authentication requirements, and any compensating controls.
- Describe any use of digital or electronic signatures and the standards used. Discuss the key management procedures for key generation, distribution, storage, and disposal.

SIGNIFICANCE IN THE SFA ENVIRONMENT:

Access control and individual accountability are important goals in any system, but particularly so in systems that process, store, and transmit sensitive information. Attempts to gain unauthorized access and acts by disgruntled or unethical users are a growing concern in government and industry. However, the greater threat is human error; well-intentioned people who make mistakes that compromise privacy and security. In either case, it is important for system management to be able to have confidence that unauthorized users cannot access sensitive systems and data, and that mechanisms are in place to track down the source of problems quickly to prevent further data compromise or corruption. As noted above, the interconnected nature of SFA systems makes the ability to control access and maintain individual accountability all the more important. See the discussion of [logical access controls](#) below.

Current Status:

Available evidence indicates that security policies standards, procedures and guidelines relating to I&A do not exist or are not implemented effectively.

Opportunities for Improvement:

Articulate policies standards, procedures and guidelines to govern I&A processes and mechanism consistently across all SFA systems. If user IDs and passwords continue to be the preferred I&A mechanism, then document and implement standards for the issues listed immediately above. These standards should be consistent across all applications and implemented within one year.

Logical Access Controls

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

1 [DLCD/DLSS](#)

1 [DLDS](#)

1 [FFEL](#)

1 [NSLDS](#)

1 [RFMS](#)

1 [PEPS](#)

STANDARD: [NIST SPECIAL PUB 800-14](#), [NIST SPECIAL PUB 800-18](#)

Organizations should implement logical access control based on policy made by a management official responsible for a particular system, application, subsystem, or group of systems. The policy should balance the often-competing interests of security, operational requirements, and user-friendliness. In general, organizations should base access control policy on the principle of least privilege, which states that users should be granted access only to the resources they need to perform their official functions.

- Discuss the controls in place to authorize or restrict the activities of users and system personnel within the application.
- Describe hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists [ACLs]).
- How are access rights granted? Are privileges granted based on job function?
- Describe the application's capability to establish an ACL or register.
- Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends.
- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.
- Indicate if encryption is used to prevent access to sensitive files as part of the system or application access control procedures.
- Describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Department of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

1 TIVWAN

SIGNIFICANCE IN THE SFA ENVIRONMENT:

Closely related to [identification and authentication](#) above, logical access controls are required to limit management's information privacy and security concerns. Most SFA system users have a limited need to access sensitive information, so information risk can be significantly reduced by limiting access to only those things each user requires to perform their job or receive the required level of support from the system. Enforcing the [least privilege principle](#) also reduces management's monitoring and [audit](#) challenge; with many potentially risky transactions prohibited by logical access controls

Current Status:

Available evidence indicates that security policies standards, procedures and guidelines relating to logical access do not exist or are not implemented effectively.

Opportunities for Improvement:

Articulate policies, standards, procedures and guidelines to govern logical access processes and mechanisms consistently across all SFA systems. Document and implement standards for the issues list immediately above within one year.

1 [CBS](#)

Public Access Controls

[Back to Risk Cycle Illustration](#)

1 [CPS](#)

STANDARD: [OMB A-130](#)

1 [DLCD/DLSS](#)

Permitting public access to a Federal application is an important method of improving information exchange with the public. At the same time, it introduces risks to the Federal application. To mitigate these risks, additional controls should be in place as appropriate. These controls are in addition to controls such as "firewalls" that are put in place for security of the general support system.

1 [DLOS](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

1 [FFEL](#)

SFA systems must necessarily provide an interface with institutions and individuals in order to provide the expected level of service. However, without mitigating controls, providing access for so many organizations and individuals outside of the SFA span of control would be fraught with risk to privacy, confidentiality, integrity and availability. Without public access controls in place to enforce [least privilege](#) and limit access to only those things each institution or user requires to receive the expected level of service, data would quickly become unreliable, with potentially serious consequences to other system and to individual privacy.

1 [NSLDS](#)

1 [RFMS](#)

CURRENT STATUS:

While available evidence indicates public access controls have been implemented for some systems, it is not clear that policies standards, procedures and guidelines relating to public access exist or are implemented consistently across all systems.

1 [PEPS](#)

Opportunities for Improvement:

1 [TIVWAN](#)

Articulate policies standards, procedures, and guidelines to govern public access processes and mechanisms consistently across all SFA systems. Document and implement these standards for all systems within one year. In no case should indirect, public users be able to manipulate production databases; all public interface should be through copies of production data.

Security Awareness and Training

[Back to Risk Cycle Illustration](#)

1 [CBS](#)

1 [CPS](#)

Standard: [OMB A-130](#), [NIST Special Pub 800-14](#)

1 [DLCD/DLSS](#)

Training is required for all individuals given access to the application, including members of the public. It should vary depending on the type of access allowed and the risk that access represents to the security of the application and information in it. This training will be in addition to that required for access to a support system.

1 [DLOS](#)

A computer security awareness and training program should encompass the following seven steps:

1 [FFEL](#)

- Identify Program Scope, Goals, and Objectives.
- Identify Training Staff
- Identify Target Audiences
- Motivate Management and Employees.
- Administer the Program
- Maintain the Program.
- Evaluate the Program.

1 [NSLDS](#)

1 [RFMS](#)

SIGNIFICANCE IN THE SFA ENVIRONMENT:

1 [PEPS](#)

Training is a key activity in the risk management process, and a challenge for SFA. This challenge stems from the geographic dispersion of SFA system managers, operators, developers, and users. Additionally, within this group security responsibilities are quite diverse. Some privacy and security issues must be understood by everyone, regardless of their position or function; system [rules of behavior](#) probably represent the irreducible minimum for the vast majority of the audience. However, many members of the system population have additional requirements and responsibilities, depending on individual job function. For example, SFA managers must become cognizant of their role in creating and fostering a secure environment at SFA and how privacy and security support SFA's operations and missions. Management must be made aware of their responsibility to provide a SFA-wide security vision, demonstrate management commitment to privacy and security, establish and resource an information security management structure, and sponsor an effective security training and awareness program. In contrast, the training provided to developers and other privileged users might emphasize understanding the SFA information privacy and security policy and standards architecture—describing the policies that affect them in their jobs, explaining their particular responsibilities, such as remaining aware of who is covered by policy, complying with policy, reporting violations, and using common sense.

1 [TIVWAN](#)

Current Status:

Available evidence suggests that the state of security training and awareness is low across the surveyed systems.

- Many SSOs are functionally unqualified and rely exclusively on their contractors (see discussion of [central security focus](#))
- There is no evidence that SFA and contractors receive regular, consistent security training
- Management awareness of federal privacy and security requirements, as well as the business advantages of implementing controls, is low.

Opportunities for Improvement:

Generally, implement the seven-step program suggested by NIST. However, the first goal should be to ensure that SSOs are properly trained and qualified and then used to implement an enterprise-wide security training and awareness program. See the [Recommendations](#) section below.

Audit Trails

[Back to Risk Cycle Illustration](#)

I [CBS](#)

I [CPS](#)

Standard: [NIST Special Pub 800-14](#)

I [DLCD/DLSS](#)

In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish *several* security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. Audit trails should be used for the following:

I [DLOS](#)

- Individual Accountability
- Reconstruction of Events
- Intrusion Detection
- Problem Identification

I [FFEL](#)

I [NSLDS](#)

An audit trail should include sufficient information to establish what events occurred and who (or what) caused them. Defining the scope and contents of the audit trail should be done carefully to balance security needs with possible performance, privacy, or other costs.

I [RFMS](#)

Organizations should protect the audit trail from unauthorized access. The following precautions should be taken:

I [PEPS](#)

- Access to online audit logs should be strictly controlled.
- Organizations should try to separate the duties of setting access controls function and audit trail administration.
- Audit trail information should be protected, for example, if it records personal information about users.

I [TIVWAN](#)

Audit trails should be reviewed periodically. The following should be considered when reviewing audit trails:

- Reviewers need to understand what normal activity looks like.
- Audit trail review can be easier if the audit trail function can be queried by some set of parameters; e.g., User ID, Terminal ID
- Administrators should review the audit trails following a known problem, violation, or unexplained event.
- Cognizant managers should determine how much review of audit trail records is necessary.
- Organizations should use audit reduction tools.

SIGNIFICANCE IN THE SFA ENVIRONMENT:

Audit is another key activity in the GAO risk management process. In order to manage risk in a dynamic environment such as SFA's, managers must be able to assess the effectiveness of risk mitigation controls, and make adjustments as required to contain costs, reduce errors, achieve efficiencies, or contain risk. Managers must have a reasonable and rational basis for making these decisions, and monitoring for control compliance and effectiveness is the best way to achieve this goal.

Effective audit requires more than simply turning on audit logs. Most systems are now capable of producing audit logs of such length and detail that the output from a single system could keep several knowledgeable staff members occupied full time reviewing them. Since this is not practical in the SFA environment, SFA must find a way to reduce the audit burden to a manageable level – no more than can be reviewed effectively by the system SSO in a fraction of that person's available hours.

Achieving this goal enables several other key risk management activities:

- Incident response: timely review of audit logs can trigger timely response to errors and hostile activity
- Risk assessment: collecting statistics of key high-risk events provides management with a quantitative basis for risk management
- Security awareness: a better understanding of where risk is actually incurred can improve the quality of security training

Current Status:

There is little evidence that audit logs are being utilized effectively to assist SFA system management determine how well users are adhering to whatever rules of behavior have been articulated. Previous years' control and security reviews indicate that if audit records are kept, they are not examined on a routine basis. Lacking this information, SFA system managers lack a basis for making risk management decisions. Current system responses indicate that while some systems make an attempt to review audit logs on a regular basis, other systems place little emphasis on collecting information to support a compliance program.

Recent (July 2000) implementation of *Real Secure* intrusion detection software at the Meriden VDC facility should improve SFA's ability to detect attempts at unauthorized access, although much depends on how the *Real Secure* modules are implemented and used.

Opportunities for Improvement:

As noted above, effective audit requires more than simply turning on audit logs. The following activities must be performed to make audit an effective tool in the risk management process.

- For each system or subsystem, identify/develop metrics for measuring high-risk events. These may be events that indicate error (e.g., attempting to enter information in a field that exceeds a range limitation) or potentially hostile activity (e.g., attempts to access restricted files).
- Set clipping levels.
- Use existing system audit tools to capture high-risk events.
- Ensure the results of measurement activities are assessed at the individual system *and* enterprise level.

For further information, see the *Monitor and Evaluate* section of the [Recommendations](#).

CBS

[CPS](#)

[DLCD/DLSS](#)

[DLOS](#)

[FFEL](#)

[NSLDS](#)

[RFMS](#)

[PEPS](#)

[TIVWAN](#)

CBS Issue	Current Status	Standard	Observations	Opportunities for Improvement
General Description/Purpose	λ	NIST Special Pub 800-18	The standard is currently being met. Documented most recently in the CBS OMB A-130 System Security Report, January 22, 1999.	Ensure complete and accurate descriptions, including detailed network and business process diagrams, are included in the CBS system security plan. See the Recommendations section for additional details.
Central Security Focus/Assigned Responsibility	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met partially. There is no appointment letter for the ACSO. The ACSO has limited security training.	Ensure the CBS SSO is properly trained and qualified. See the section on security training and awareness , and the related recommendations for the Promote Awareness phase of the risk management cycle. In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.
System Environment	λ	NIST Special Pub 800-18	The standard is currently being met.	See the recommendation for General Description/Purpose above.
System Interconnection/Information Sharing	λ	NIST Special Pub 800-18	The standard is not currently being met. CBS does not have MOUs or MOAs that govern its connection to TIVWAN.	Ensure all CBS connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.
Applicable Laws and Regulations	λ	NIST Special Pub 800-18, Privacy Act, A-130 Appendix I	CBS is cognizant of applicable laws and regulations. No Privacy Act information stored on this system	N/A
Description of Information Sensitivity	λ	NIST Special Pub 800-18	The standard is currently being met.	See the Recommendations relating to developing a security model below.
Risk Assessment and Management	λ	OMB A-130	This risk assessment serves to satisfy the standard, although previously no risk assessment had been performed for CBS.	Implement the GAO risk management cycle in the CBS environment. See the other improvement suggestions for this system as well as the Conclusions and Recommendations sections.
Review of Security Controls	λ	OMB A-130	The standard is currently being met; Booz Allen Hamilton (BAH) conducted an A-130 review in 1998.	Ensure future controls reviews measure the maturity of the CBS risk management cycle.
Rules of Behavior	λ	OMB A-130	The standard is not currently being met. Rules of Behavior for CBS do not exist.	Document rules of behavior for CBS. Ensure managers and users are trained to understand them.
Security Life Cycle Planning	λ	NIST Special Pub 800-	The standard is not currently being met.	Ensure that security in the information life cycle is

CBS Issue	Current Status	Standard	Observations	Opportunities for Improvement
		18	CBS has no security plan, and management reports that life cycle security planning is largely “Not Applicable” despite the high requirement for data integrity.	addressed in CBS life cycle planning documents. See the Security Life Cycle Planning section for additional details.
Authorize Processing	λ	OMB A-130	The standard is currently being met partially. Although CBS has not sought certification, this report or the 1998 BAH A-130 report could serve as the basis for a system certification/authority to operate.	Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal CBS certification test under NIST guidance (FIPS 102).
Personnel Security	λ	OMB A-130	The standard is currently being met. However, CBS does not appear to be cognizant of ED personnel security guidance. In addition, at the operational level security decision-making authority has devolved on the UAL vendor; the CBS SSO does not appear to play a role in representing the government interest.	Implement ED personnel security guidance. See the Personnel Security section for additional details.
Physical and Environmental Protection	λ	NIST Special Pub 800-18	The standard is currently being met. CBS relies on the controls at the VDC and at Regional Office Building 3 (ROB3).	When developing/updating the CBS security plan, ensure the controls noted above are fully addressed.
Production, Input/Output Controls	λ	NIST Special Pub 800-18	The standard is not currently being met. CBS reports production controls are not required or do not exist.	Implement Security Life Cycle Planning , Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the CBS security plan.
Contingency Planning	λ	OMB A-130	The standard is currently being met partially. The ACSO did not have a copy of the contingency plan. The ACSO did not have a copy of the disaster recovery plan.	Ensure that formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the CBS SSO has a copy of all plans.
Application Software Maintenance Controls	λ	NIST Special Pub 800-18	The standard is currently being met. CBS appears to have a structured process in place for managing changes to system software.	Examine ED guidance relating to system life cycle planning. Ensure that CBS CM processes and procedures are consistent with that guidance, and that the CBS SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.
Data Integrity/Validation Controls	λ	NIST Special Pub 800-18	The standard is not currently being met. There was no evidence of controls for assuring the integrity and validity of the data.	Ensure CBS complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details
Documentation	λ	NIST Special Pub 800-18	The standard is currently being met partially. While CBS does maintain some software/application	Develop a NIST-compliant (Special Pub 800-18) security plan for CBS. See the Recommendations

CBS Issue	Current Status	Standard	Observations	Opportunities for Improvement
			<p>documentation, functional requirements, and system test results, many other required documents are missing. These include:</p> <ul style="list-style-type: none"> ● vendor hardware documentation ● major application security plan ● standard operating procedures ● emergency procedures ● contingency plans ● user rules/procedures ● risk assessment ● certification/accreditation statements/documents ● verification reviews/site inspections 	<p>section for additional details.</p>
<p>Identification and Authentication</p>	<p>λ</p>	<p>NIST Special Pub 800-14, NIST Special Pub 800-18</p>	<p>The standard is currently being met partially. CBS features some automated password standard enforcement, but several limitations were reported.</p> <p>Passwords lengths as short as 4 characters are allowed; 6 character should be the minimum.</p> <p>Passwords are currently alpha characters only; numbers and special characters should be allowed.</p> <p>There is currently no restriction on the frequency of change; this allows users to easily bypass the 3-generation password history. Passwords should have a minimum time limit of 30 days.</p>	<p>Ensure CBS complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.</p>
<p>Logical Access Controls</p>	<p>λ</p>	<p>NIST Special Pub 800-14, NIST Special Pub 800-18</p>	<p>The standard is currently being met partially. At the application level CBS has a simple individual-based access control matrix; access options are read-only, read/update, or administrator (all access). These permissions are associated with individual user IDs and protected by a password dialogue. Network access is controlled by the TIVWAN and EDNET authorities, not by CBS management.</p> <p>Nonetheless, several limitations were noted over and above the password standards concerns noted above. These include:</p> <ul style="list-style-type: none"> ● There was no evidence of policies for defining the logical access control process, or procedures for monitoring it ● There are no lockouts and logouts when a user 	<p>Document and implement within one year CBS-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.</p>

CBS Issue	Current Status	Standard	Observations	Opportunities for Improvement
			<p>leaves a terminal</p> <ul style="list-style-type: none"> No log-on banner alerts users that their actions may be monitored <p>In addition, there was no evidence that concerns from previous risk assessments and control reviews had been addressed. These include:</p> <ul style="list-style-type: none"> RACF's automatic account revocation capability is not activated There are no special protections assigned to the Default Reduction Assistance Program (DRAP) database Protect -all option has not been activated Batchallracf has not been activated Tape data set protection has not been activated All users have Time Sharing Option (TSO) access 	
Public Access Controls	λ	OMB A-130	The standard is currently being met; CBS has no direct public interface.	Ensure all CBS-specific policies, standards, procedures and guidelines to govern public access processes and mechanisms are properly documented.
Security Awareness and Training	λ	OMB A-130, NIST Special Pub 800-14	The standard is not currently being met. While CBS reports they are aware of ED security training requirements, they do not report actually attending it. This is of particular concern for the CBS SSO, who is new to his position and does not have a security background.	Provide security training for the CBS SSO; once trained, the CBS SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.
Audit Trails	λ	NIST Special Pub 800-14	The standard is currently being met, however, audit logs are only inspected when a problem occurs rather than monitored on a regular basis as part of a risk management program.	Ensure CBS audit results are being used effectively to help CBS managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.

CPS

[CBS](#)

[DLCD/DLSS](#)

[DLOS](#)

[FFEL](#)

[NSLDS](#)

[RFMS](#)

[PEPS](#)

[TIVWAN](#)

CPS Issue	Current Status	Standard	Current Status	Opportunities for Improvement
General Description/Purpose	λ	NIST Special Pub 800-18	The standard is currently being met. Documented most recently in the CPS OMB A-130 System Security Report, November 3, 1998.	Ensure complete and accurate descriptions, including detailed network and business process diagrams, are included in the CPS system security plan. See the Recommendations section for additional details.
Central Security Focus/Assigned Responsibility	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met partially. The ACSO position is not a full-time position. The ACSO and OPE CSO are not always kept informed of security issues that may affect their systems or their operations. The ACSO has no contact with the contractor security personnel. The CPS COTR performs many of the ACSO functions The ACSO has not received technical security training.	Ensure the CBS SSO is properly trained and qualified. See the section on security training and awareness , and the related recommendations for the Promote Awareness phase of the risk management cycle. In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.
System Environment	λ	NIST Special Pub 800-18	The standard is currently being met.	See the recommendation for General Description/Purpose above.
System Interconnection/Information Sharing	λ	NIST Special Pub 800-18	The standard is not currently being met. There was no evidence identifying whether or not CPS interfaces with other SFA systems or external entities.	Ensure all CPS connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.
Applicable Laws and Regulations	λ	NIST Special Pub 800-18, Privacy Act, A-130 Appendix I	CPS is cognizant of applicable laws and regulations. The status of Privacy Act compliance is unknown. Although this system presumably complies with notice, publication, and annual/biennial/quadrennial review requirements, as those remain the responsibility of the Department's Chief Privacy Officer, no system-specific information with regard to access controls, storage, retrieval, retention, disclosure logging, contractor compliance, disposal of records, or employee training was provided for these systems.	N/A
Description of Information Sensitivity	λ	NIST Special Pub 800-18	The standard is currently being met.	See the Recommendations relating to developing a security model below.

CPS Issue	Current Status	Standard	Current Status	Opportunities for Improvement
				security model below.
Risk Assessment and Management	λ	OMB A-130	The standard is not currently being met. No risk assessment has been performed for CPS	Implement the GAO risk management cycle in the CPS environment. See the other improvement suggestions for this system as well as the Conclusions and Recommendations sections.
Review of Security Controls	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Ensure future controls reviews measure the maturity of the CPS risk management cycle.
Rules of Behavior	λ	OMB A-130	The standard is not currently being met. Rules of behavior for CPS are not documented in detail.	Document rules of behavior for CPS. Ensure that managers and users are trained to understand them.
Security Life Cycle Planning	λ	NIST Special Pub 800-18	The standard is not currently being met. There was no evidence of appropriate security controls for each phase of the System Development Life Cycle.	Ensure (as appropriate) privacy and security in the information life cycle are addressed in CPS life cycle planning documents. See the Security Life Cycle Planning section for additional details.
Authorize Processing	λ	OMB A-130	The standard is not currently being met. Although CPS has not sought certification, this report could serve as the basis for a system certification/ authority to operate.	Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal CPS certification test under NIST guidance (FIPS 102).
Personnel Security	λ	OMB A-130	The standard is currently being met.	Implement ED personnel security guidance. See the Personnel Security section for additional details.
Physical and Environmental Protection	λ	NIST Special Pub 800-18	The standard is currently being met.	When developing/updating the CPS security plan, ensure the controls noted above are fully addressed.
Production, Input/Output Controls	λ	NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of controls for the installation and use of the application.	Implement Security Life Cycle Planning , Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the CPS security plan.
Contingency Planning	λ	OMB A-130	The standard is currently being met partially. The ACSO did not have a copy of the contingency plan. The ACSO did not have a copy of the disaster recovery plan. NCS has no formal procedures for dealing with security incidents.	Ensure formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the CPS SSO has a copy of all plans.
Application Software Maintenance Controls	λ	NIST Special Pub 800-18	The standard is not currently being met. There was no evidence of controls for the maintenance of the application.	Examine ED guidance relating to system life cycle planning. Ensure that CPS CM processes and procedures are consistent with that guidance, and that the CPS SSO is integrated into the systems development

CPS Issue	Current Status	Standard	Current Status	Opportunities for Improvement
				the CPS SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.
Data Integrity/Validation Controls	λ	NIST Special Pub 800-18	The standard is not currently being met. There was no evidence of controls for assuring the integrity and validity of the data.	Ensure CPS complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details
Documentation	λ	NIST Special Pub 800-18	The standard is currently being met partially. There is no current and approved CPS security plan.	Develop a NIST-compliant (Special Pub 800-18) security plan for CPS. See the Recommendations section for additional details.
Identification and Authentication	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of policies for defining the password management process or procedures for monitoring it. TIVWAN passwords are stored in clear text (uncompressed) on two occasions during the password change process. FAFSA employees have access to a password database. Passwords are not as strong as good business practices warrant.	Ensure CPS complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.
Logical Access Controls	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of policies for defining the logical access control process, or procedures for monitoring it. RACF's automatic account revocation capability may not be activated. Unsecured E-Mail used for requesting new CPS accounts. The ACSO has no active role in user account management. Sensitive information contained in documentation or other media is not identified clearly with an external label or other markings. No log-on banner alerts users their actions may be	Document and implement within one year CPS-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.

CPS Issue	Current Status	Standard	Current Status	Opportunities for Improvement
			monitored. Although the ACSO participates in the CPS CM process, this participation is in capacities other than security.	
Public Access Controls	λ	OMB A-130	The standard is currently being met.	Ensure all CPS-specific policies, standards, procedures and guidelines to govern public access processes and mechanisms are properly documented.
Security Awareness and Training	λ	OMB A-130, NIST Special Pub 800-14	The standard is not currently being met. There was no evidence of policies or procedures for implementing a security awareness program. Security awareness training has not been implemented.	Provide security training for the CPS SSO; once trained, the CPS SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.
Audit Trails	λ	NIST Special Pub 800-14	The standard is currently being met partially. The Department does not review audit logs. NCS does not provide quarterly reports of extracted audit data	Ensure CPS audit results are being used effectively to help CPS managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.

DLCD/DLSS

[CBS](#)

[CPS](#)

[DLOS](#)

[FFEL](#)

[NSLDS](#)

[RFMS](#)

[PEPS](#)

[TIVWAN](#)

DLCD/DLSS Issue	Current Status	Standard	Comments	Opportunities for Improvement
General Description/Purpose	λ	NIST Special Pub 800-18	The standard is currently being met. Documented most recently in the DLSS Sensitive Application Certification Review Report, May 1996.	Ensure complete and accurate descriptions, including detailed network and business process diagrams, are included in the DLCD/DLSS system security plan. See the Recommendations section for additional details.
Central Security Focus/Assigned Responsibility	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met partially.	Ensure the CBS SSO is properly trained and qualified. See the section on security training and awareness , and the related recommendations for the Promote Awareness phase of the risk management cycle. In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.
System Environment	λ	NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of a technical description of the system.	See the recommendation for General Description/Purpose above.
System Interconnection/Information Sharing	λ	NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of Memoranda of Understanding (MOU), or Trading Partner Agreements (TPA), or that the interfaces had been addressed in the Security Plan.	Ensure all DLCD/DLSS connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.
Applicable Laws and Regulations	λ	NIST Special Pub 800-18, Privacy Act, A-130 Appendix I	DLCD/DLSS is cognizant of applicable laws and regulations. The status of Privacy Act compliance is unknown. Although this system presumably complies with notice, publication, and annual/biennial/quadrennial review requirements, as those remain the responsibility of the Department's Chief Privacy Officer, no system-specific information with regard to access controls, storage, retrieval, retention, disclosure logging, contractor compliance, disposal of records, or employee training was provided for these systems.	N/A
Description of Information Sensitivity	λ	NIST Special Pub 800-18	The standard is currently being met.	See the Recommendations relating to developing a security model below.
Risk Assessment and Management	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Implement the GAO risk management cycle in the DLCD/DLSS environment. See the other improvement suggestions for this system as well as the Conclusions

DLCD/DLSS Issue	Current Status	Standard	Comments	Opportunities for Improvement
				and Recommendations sections.
Review of Security Controls	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Ensure future controls reviews measure the maturity of the DLCD/DLSS risk management cycle.
Rules of Behavior	λ	OMB A-130	The standard is not currently being met. There was no evidence that the Rules of Behavior were documented.	Document rules of behavior for DLCD/DLSS. Ensure managers and users are trained to understand them.
Security Life Cycle Planning	λ	NIST Special Pub 800-18	The standard is not currently being met. There was no evidence of appropriate security controls for each phase of the System Development Life Cycle.	Ensure that (as appropriate) privacy and security in the information life cycle are addressed in DLCD/DLSS life cycle planning documents. See the Security Life Cycle Planning section for additional details.
Authorize Processing	λ	OMB A-130	The standard is not currently being met. There was no evidence that DLCD/DLSS had been certified and accredited. Although DLCD/DLSS has not sought certification, this report could serve as the basis for a system certification/ authority to operate.	Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal DLCD/DLSS certification test under NIST guidance (FIPS 102).
Personnel Security	λ	OMB A-130	The standard is currently being met partially. Management of security clearance processing needed improvement (e.g., "...require any personnel not cleared to submit the required paperwork...", "...inform personnel, particularly program management, of the results of clearance processing...").	Implement ED personnel security guidance. See the Personnel Security section for additional details.
Physical and Environmental Protection	λ	NIST Special Pub 800-18	The standard is currently being met partially. Security enhancements were needed (e.g., visitors needed positive identification, establish a sign-in log, etc.).	When developing/updating the DLCD/DLSS security plan, ensure the controls noted above are fully addressed.
Production, Input/Output Controls	λ	NIST Special Pub 800-18	The standard is currently being met.	Implement Security Life Cycle Planning , Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the DLCD/DLSS security plan.
Contingency Planning	λ	OMB A-130	The standard is currently being met.	Ensure formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the DLCD/DLSS SSO has a copy of all plans.
Application Software Maintenance Controls	λ	NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of controls for the maintenance	Examine ED guidance relating to system life cycle planning. Ensure that DLCD/DLSS CM processes and

DLCD/DLSS Issue	Current Status	Standard	Comments	Opportunities for Improvement
			of the application.	procedures are consistent with that guidance, and that the DLCD/DLSS SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.
Data Integrity/Validation Controls	λ	NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of controls for assuring the integrity and validity of the data.	Ensure DLCD/DLSS complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details.
Documentation	λ	NIST Special Pub 800-18	The standard is currently being met partially. Disaster Recovery Plan (DRP) needed to be updated to reflect changes. The Security Plan needed to be updated based upon a recent revision of OMB Circular A-130.	Develop a NIST-compliant (Special Pub 800-18) security plan for DLCD/DLSS. See the Recommendations section for additional details.
Identification and Authentication	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	The standard is currently being met.	Ensure DLCD/DLSS complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.
Logical Access Controls	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	The standard is currently being met.	Ensure all DLCD/DLSS-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms are documented in the DLCD/DLSS security plan.
Public Access Controls	λ	OMB A-130	The standard is currently being met partially. There was no evidence documenting whether or not public access was allowed to DLCD/DLSS.	Document and implement within one year DLCD/DLSS-specific policies, standards, procedures and guidelines to govern public access processes and mechanisms.
Security Awareness and Training	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met partially. More in -depth training needed to be provided to additional personnel.	Provide security training for the DLCD/DLSS SSO; once trained, the DLCD/DLSS SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.
Audit Trails	λ	NIST Special Pub 800-14	The standard is currently being met partially. There was no evidence to indicate that the audit trails were being reviewed by appropriate staff.	Ensure DLCD/DLSS audit results are being used effectively to help DLCD/DLSS managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.

DLOS

[CBS](#)

[CPS](#)

[DLCD/DLSS](#)

[FFEL](#)

[NSLDS](#)

[RFMS](#)

[PEPS](#)

[TIVWAN](#)

DLOS Issue	Current Status	Standard	Comments	Opportunities for Improvement
General Description/Purpose	λ	NIST Special Pub 800-18	The standard is currently being met.	Ensure the description provided in the DLOS submission for this report is included in the DLOS system security plan. The plan should also include detailed network and business process diagrams. See the Recommendations section for additional details.
Central Security Focus/Assigned Responsibility	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met partially.	Ensure the CBS SSO is properly trained and qualified. See the section on security training and awareness , and the related recommendations for the Promote Awareness phase of the risk management cycle. In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.
System Environment	λ	NIST Special Pub 800-18	The standard is currently being met.	See the recommendation for General Description/Purpose above.
System Interconnection/Information Sharing	λ	NIST Special Pub 800-18	The standard is currently being met partially. While interface specifications are reported to exist for all systems that are directly connected, there was no evidence of Memoranda of Understanding (MOU), or Trading Partner Agreements (TPAs).	Ensure all system connections and information sharing with non-SFA entities are codified in the DLSO security plan. See the section above on system interconnection and information sharing for further details.
Applicable Laws and Regulations	λ	NIST Special Pub 800-18, Privacy Act, A-130 Appendix I	DLOS is cognizant of applicable laws and regulations. Regarding the Privacy Act, DLOS has one system of records, however a System of Records Notice (SORN) has apparently not been submitted. Privacy Act data includes name, address, birthdate, social security number, demographic, financial, statistical information and financial data. Information is retrieved by social security number (SSN). No alterations have been made to the system of records. DLOS has implemented and documented policies and procedures for access of records in accordance with Privacy Act requirements, but it is unclear from	Publish/update a LOS SORN. Create/formalize policies and procedures for storage, retrieval, retention, and disposal of Privacy Act information. Ensure the contract with EDS requires contractors to comply with Privacy Act requirements. There was no evidence that DLOS personnel participate in annual Department of Education training on security and Privacy Act requirements.

DLOS Issue	Current Status	Standard	Comments	Opportunities for Improvement
			<p>available evidence if similar policies and procedures exist for storage, retrieval, retention, and disposal.</p> <p>DLOS does not participate in any matching program with any other agency.</p> <p>There is no evidence that the contract with EDS requires contractors to comply with Privacy Act requirements.</p> <p>While training on security, including privacy act requirements, is supposed to be provided to all Department of Education employees and contractors annually, there was no evidence that DLOS personnel participate in such training.</p> <p>Disclosures of Privacy Act information are made by telephone to participating individuals or their authorized representatives in accordance with the system's published routine use. No logs of date, time, and content of the phone calls are maintained. Applicants are given direct access to their data through this system. It is not clear how DLOS ensures that individual records are accurate through such mechanisms as editing software, software testing, or SFA testing and review. Only the institution of record can make changes to the data unless a request, in writing, is sent to the Loan Origination Center (LOC) for manual update by LOC personnel.</p>	
Description of Information Sensitivity	λ	NIST Special Pub 800-18	<p>The standard is not currently being met.</p> <p>There was no evidence of assigned values for the protection requirements (e.g., high, medium, low).</p>	See the Recommendations relating to developing a security model below.
Risk Assessment and Management	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Implement the GAO risk management cycle in the DLOS environment. See the other improvement suggestions for this system as well as the Conclusions and Recommendations sections.
Review of Security Controls	λ	OMB A-130	The standard is currently being met; at least four control and operational reviews have been conducted on various parts of the DLOS within the last two years.	Ensure future controls reviews measure the maturity of the DLOS risk management cycle.
Rules of Behavior	λ	OMB A-130	The standard is not currently being met. There was no evidence that the Rules of Behavior are documented for DLOS.	Document rules of behavior for DLOS. Ensure managers and users are trained to understand them.

DLOS Issue	Current Status	Standard	Comments	Opportunities for Improvement
			DLOS.	
Security Life Cycle Planning	λ	NIST Special Pub 800-18	The standard is not currently being met. There was no evidence of appropriate security controls for each phase of the System Development Life Cycle.	Ensure that (as appropriate) privacy and security in the information life cycle are addressed in DLOS life cycle planning documents. See the Security Life Cycle Planning section for additional details
Authorize Processing	λ	OMB A-130	The standard is not currently being met. While this report and/or the operational/security controls reviews conducted in the past two years could potentially serve as a basis for certification, there was no evidence that DLOS has sought certification or authority to operate.	Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal DLOS certification test under NIST guidance (FIPS 102).
Personnel Security	λ	OMB A-130	The standard is currently being met. EDS performs its own personnel background checks, and ED performs its own checks for staff occupying sensitive positions. In addition, EDS, the DLSO vendor, has implemented policies and procedures for segregation of duties, ethics, and termination.	N/A
Physical and Environmental Protection	λ	NIST Special Pub 800-18	The standard is currently being met. EDS has physical access, environmental and fire safety controls at facilities it controls. DLOS operations at the VDC are protected by systems and procedures at that site.	When developing/updating the DLOS security plan, ensure the controls noted opposite are fully described.
Production, Input/Output Controls	λ	NIST Special Pub 800-18	The standard is currently being met. Automated and manual controls have been implemented for processing, storage, and output from the Loan Origination and Loan Consolidation subsystems.	Implement Security Life Cycle Planning , Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the DLOS security plan.
Contingency Planning	λ	OMB A-130	The standard is currently being met.	Ensure formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the DLOS SSO has a copy of all plans.
Application Software Maintenance Controls	λ	NIST Special Pub 800-18	The standard is currently being met.	Examine ED guidance relating to system life cycle planning. Ensure that DLOS CM processes and procedures are consistent with that guidance, and that the DLOS SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.

DLOS Issue	Current Status	Standard	Comments	Opportunities for Improvement
Data Integrity/Validation Controls	λ	NIST Special Pub 800-18	The standard is currently being met.	Ensure DLOS complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details.
Documentation	λ	NIST Special Pub 800-18	The standard is currently being met. DLOS appears to be exceptionally well documented; the only documentation that is lacking is associated with the certification and accreditation cycle, see above .	Ensure the DLOS security plan is NIST-compliant.
Identification and Authentication	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	The standard is currently being met. Of note, current standards call for password changes every 30 days. While this is acceptable, frequent password change may lead users to select weak passwords or serial passwords due to the frequency of change. In addition, it is not clear why some parts of the system lock users out after 3 failed login attempt and another locks out after six.	Ensure DLOS complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.
Logical Access Controls	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	The standard is currently being met. DLOS has implemented policies and procedures to govern system access and permissions.	Ensure DLOS-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms are documented in the DLOS security plan.
Public Access Controls	λ	OMB A-130	The standard is currently being met.	Ensure DLOS-specific policies, standards, procedures and guidelines to govern public access processes and mechanisms via web interfaces are documented in the DLOS security plan.
Security Awareness and Training	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met, with the following reservation: all current training is by and for the EDS vendor; there is no evidence that government staff are receiving equivalent training. In addition, there is no assurance that federal and ED security standards are being covered in vendor training.	Provide security training for the DLOS SSO; once trained, the DLOS SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.
Audit Trails	λ	NIST Special Pub 800-14	The standard is currently being met, however, audit logs are only inspected when a problem occurs rather than monitored on a regular basis as part of a risk management program.	Ensure DLOS audit results are being used effectively to help DLOS managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.

FFEL

[CBS](#)

[CPS](#)

[DLCD/DLSS](#)

[DLOS](#)

[NSLDS](#)

[RFMS](#)

[PEPS](#)

[TIVWAN](#)

FFEL Issue	Current Status	Standard	Comments	Opportunities for Improvement
General Description/Purpose	λ	NIST Special Pub 800-18	The standard is currently being met. Documented most recently in the FFEL Sensitive Application Certification Review Report, July 1996.	Ensure complete and accurate descriptions, including detailed network and business process diagrams, are included in the FFEL system security plan. See the Recommendations section for additional details.
Central Security Focus/Assigned Responsibility	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met partially.	Ensure the CBS SSO is properly trained and qualified. See the section on security training and awareness , and the related recommendations for the Promote Awareness phase of the risk management cycle. In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.
System Environment	λ	NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of a technical description of the system.	See the recommendation for General Description/Purpose above.
System Interconnection/Information Sharing	λ	NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of Memoranda of Understanding (MOU), or Trading Partner Agreements (TPA), or that the interfaces had been addressed in the Security Plan.	Ensure all FFEL connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.
Applicable Laws and Regulations	λ	NIST Special Pub 800-18, Privacy Act, A-130 Appendix I	FFEL is cognizant of applicable laws and regulations. The status of Privacy Act compliance is unknown. Although this system presumably complies with notice, publication, and annual/biennial/quadrennial review requirements, as those remain the responsibility of the Department's Chief Privacy Officer, no system-specific information with regard to access controls, storage, retrieval, retention, disclosure logging, contractor compliance, disposal of records, or employee training was provided for these systems.	N/A
Description of Information Sensitivity	λ	NIST Special Pub 800-18	The standard is currently being met.	See the Recommendations relating to developing a security model below.
Risk Assessment and	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Implement the GAO risk management cycle in the FFEL

FFEL Issue	Current Status	Standard	Comments	Opportunities for Improvement
Management				environment. See the other improvement suggestions for this system as well as the Conclusions and Recommendations sections.
Review of Security Controls	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Ensure future controls reviews measure the maturity of the FFEL risk management cycle.
Rules of Behavior	λ	OMB A-130	The standard is not currently being met. There was no evidence that the Rules of Behavior were documented.	Document rules of behavior for FFEL. Ensure managers and users are trained to understand them.
Security Life Cycle Planning	λ	NIST Special Pub 800-18	The standard is not currently being met. There was no evidence of appropriate security controls for each phase of the System Development Life Cycle.	Ensure that (as appropriate) privacy and security in the information life cycle are addressed in FFEL life cycle planning documents. See the Security Life Cycle Planning section for additional details
Authorize Processing	λ	OMB A-130	The standard is not currently being met. Although FFEL has not sought certification, this report could serve as the basis for a system certification/ authority to operate.	Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal FFEL certification test under NIST guidance (FIPS 102).
Personnel Security	λ	OMB A-130	The standard is currently being met partially. Security clearance processing management needed improvement. Uniform and consistent personnel security policies should be implemented at all E-Systems locations associated with FFEL.	Implement ED personnel security guidance. See the Personnel Security section for additional details.
Physical and Environmental Protection	λ	NIST Special Pub 800-18	The standard is currently being met partially. Security enhancements were needed (e.g., require employees to display identification, provide safety training, secure items of value in locking cabinets, etc.).	When developing/updating the FFEL security plan, ensure the controls noted above are fully addressed.
Production, Input/Output Controls	λ	NIST Special Pub 800-18	The standard is currently being met.	Implement Security Life Cycle Planning , Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the FFEL security plan.
Contingency Planning	λ	OMB A-130	The standard is currently being met partially. Develop a Disaster Recovery Plan (DRP) and Continuity of Operations Plan for the Ballston facility. Disaster Recovery Plan (DRP) has not been kept current.	Ensure formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the FFEL SSO has a copy of all plans.

FFEL Issue	Current Status	Standard	Comments	Opportunities for Improvement
Application Software Maintenance Controls	λ	NIST Special Pub 800-18	The standard is currently being met partially. Application development/testing processes needed to be reviewed. SSO role had not been formalized in the Configuration Management (CM) process.	Examine ED guidance relating to system life cycle planning. Ensure FFEL CM processes and procedures are consistent with that guidance, and that the FFEL SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.
Data Integrity/Validation Controls	λ	NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of controls for assuring the integrity and validity of the data.	Ensure FFEL complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details.
Documentation	λ	NIST Special Pub 800-18	The standard is currently being met partially. Security Plan needed to be updated based upon a recent revision of OMB Circular A-130.	Develop a NIST-compliant (Special Pub 800-18) security plan for FFEL. See the Recommendations section for additional details.
Identification and Authentication	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence that password usage was being managed/monitored.	Ensure FFEL complies with SFA standards for data user IDs and passwords. See the Identification and Authentication section above for detailed guidance.
Logical Access Controls	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	Documented most recently in the FFEL Sensitive Application Certification Review Report, July 1996. Ensure that individual accountability is established and maintained for the LAN development activities.	Document and implement within one year FFEL-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.
Public Access Controls	λ	OMB A-130	The standard is currently being met partially. There was no evidence documenting whether or not public access was allowed to FFEL.	Document and implement within one year FFEL-specific policies, standards, procedures and guidelines to govern public access processes and mechanisms.
Security Awareness and Training	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met partially. Security awareness training needed to be improved for ED staff, and in-depth training needed to be provided to additional personnel.	Provide security training for the FFEL SSO; once trained, the FFEL SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.
Audit Trails	λ	NIST Special Pub 800-14	The standard is currently being met partially. There was no evidence to indicate the audit trails were being reviewed by appropriate staff.	Ensure FFEL audit results are being used effectively to help FFEL managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.

NSLDS

[CBS](#)

[CPS](#)

[DLCD/DLSS](#)

[DLOS](#)

[FFEL](#)

[RFMS](#)

[PEPS](#)

[TIVWAN](#)

NSLDS Issue	Current Status	Standard	Observations	Opportunities for Improvement
General Description/Purpose	λ	NIST Special Pub 800-18	The standard is currently being met. Documented most recently in the NSLDS OMB A-130 System Security Report, July 8, 1998, and NIST 800-18 Questionnaire, 8/11/00.	Ensure complete and accurate descriptions, including detailed network and business process diagrams, are included in the NSLDS system security plan. See the Recommendations section for additional details.
Central Security Focus/Assigned Responsibility	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met partially. ACSO is not a full-time position. ACSO has not received technical training regarding NSLDS security. Data ownership has not been defined clearly. CSO and ACSO were not involved directly in addressing certain key decisions affecting the NSLDS security. Provisions of the Department's security and procurement policy were not followed in awarding NSLDS contract.	Ensure the CBS SSO is properly trained and qualified. See the section on security training and awareness , and the related recommendations for the Promote Awareness phase of the risk management cycle. In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.
System Environment	λ	NIST Special Pub 800-18	The standard is currently being met.	See the recommendation for General Description/Purpose above.
System Interconnection/Information Sharing	λ	NIST Special Pub 800-18	The standard is not currently being met. Despite the numerous interfaces to NSLDS, system managers do not feel MOUs or MOAs are applicable.	Ensure all NSLDS connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.
Applicable Laws and Regulations	λ	NIST Special Pub 800-18, Privacy Act, A-130 Appendix I	CBS is cognizant of applicable laws and regulations. Regarding the Privacy Act: although this system presumably complies with notice, publication, and annual/biennial/quadrennial review requirements, NSLDS management did not respond to the questionnaire provided on 6 Jul 00, so the system's current compliance posture is unknown.	N/A
Description of Information Sensitivity	λ	NIST Special Pub 800-18	The standard is currently being met.	See the Recommendations relating to developing a security model below.

NSLDS Issue	Current Status	Standard	Observations	Opportunities for Improvement
Risk Assessment and Management	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Implement the GAO risk management cycle in the NSLDS environment. See the other improvement suggestions for this system as well as the Conclusions and Recommendations sections.
Review of Security Controls	λ	OMB A-130	The standard is currently being met; NSLDS has been the subject of several control reviews and audits in the past two years.	Ensure future controls reviews measure the maturity of the NSLDS risk management cycle.
Rules of Behavior	λ	OMB A-130	The standard is currently being met in the strictest sense; users are provided with a copy of and extract from the Privacy Act – a worthy practice. However, this does not cover all of the system use rules that every user should understand.	Ensure managers and users are trained to understand NSLDS rules of behavior.
Security Life Cycle Planning	λ	NIST Special Pub 800-18	The standard is not currently being met. While security in the NSLDS life cycle was reported to be described in the system security plan, a copy of this plan was not provided.	Ensure that (as appropriate) privacy and security in the information life cycle are addressed in NSLDS life cycle planning documents. See the Security Life Cycle Planning section for additional details.
Authorize Processing	λ	OMB A-130	The standard is not currently being met. Although NSLDS has not sought certification, this report could serve as the basis for a system certification/authority to operate.	Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal NSLDS certification test under NIST guidance (FIPS 102).
Personnel Security	λ	OMB A-130	The standard is currently being met, although it is not clear that ED guidance is being followed.	Implement ED personnel security guidance. See the Personnel Security section for additional details.
Physical and Environmental Protection	λ	NIST Special Pub 800-18	The standard is currently being met. NSLDS benefits from the physical and environmental controls at the Meriden VDC.	When developing/updating the NSLDS security plan, ensure the controls noted above are fully addressed.
Production, Input/Output Controls	λ	NIST Special Pub 800-18	The standard is not currently being met. There was no evidence of controls for the installation and use of the application.	Implement Security Life Cycle Planning , Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the NSLDS security plan.
Contingency Planning	λ	OMB A-130	The standard is currently being met, in the sense that NSLDS relies on the Meriden VDC to handle many aspects of incident response and disaster recovery. However, this does not relieve NSLDS management of the responsibility to provide oversight of vendor provided services.	Ensure formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the NSLDS SSO has a copy of all plans.

NSLDS Issue	Current Status	Standard	Observations	Opportunities for Improvement
Application Software Maintenance Controls	λ	NIST Special Pub 800-18	The standard is currently being met.	Examine ED guidance relating to system life cycle planning. Ensure that NSLDS CM processes and procedures are consistent with that guidance, and that the NSLDS SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.
Data Integrity/Validation Controls	λ	NIST Special Pub 800-18	The standard is currently being met. NSLDS apparently has few if any automated data integrity and validation controls, as two vendors who provide quality control and reconciliation services were cited by NSLD management as the control mechanism. For other data integrity services NSLDS relies entirely on services provided by the VDC.	Ensure NSLDS complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details.
Documentation	λ	NIST Special Pub 800-18	The standard is currently being met partially. While CBS does maintain a substantial body of system documentation, several other required documents are missing. These include: <ul style="list-style-type: none"> ● functional requirements ● system test results ● user rules/procedures ● certification/accreditation statements/documents 	Ensure the NSLDS security plan is NIST -compliant.
Identification and Authentication	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	There was no evidence of policies for defining the password management process, or procedures for monitoring it, nor was there any evidence that previous discrepancies had been addressed. Users share accounts and passwords. Password expiration interval was increased to 120 days.	Ensure NSLDS complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.
Logical Access Controls	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	The standard is currently being met partially. Previous year audits indicate NSLDS needed to tighten up on some areas of logical access (see red text below). Evidence made available does not indicate these weaknesses have been addressed, nor was enough information provided to allow an assessment of the NSLDS logical access posture. RACF is used to control a role-based access schema, but the granularity of access	Document and implement within one year NSLDS-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.

NSLDS Issue	Current Status	Standard	Observations	Opportunities for Improvement
			<p>that can be achieved was not discussed.</p> <p>There is no formal process for removing terminated employees or employees who no longer need the access.</p> <p>NSLDS school users can view all loans and borrower transactions of a student via the SSN search regardless of whether or not the school was authorized by that student in his/her Free Application For Federal Student Aid (FAFSA) form.</p> <p>Changes to the NSLDS were not announced in the Federal Register.</p> <p>RACF system default UserID was not revoked.</p> <p>Security changes to the NSLDS mainframe by users with the system or group SPECIAL attribute are not reviewed by designated personnel.</p>	
Public Access Controls	λ	OMB A-130	The standard is currently being met.	Ensure NSLDS-specific policies, standards, procedures and guidelines to govern public access processes and mechanisms are properly documented in the NSLDS security plan.
Security Awareness and Training	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met partially. The description of training provided on an “as needed” basis is only marginally adequate, and suggests that NSLDS opts out of annual security and privacy training.	Provide security training for the NSLDS SSO; once trained, the NSLDS SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.
Audit Trails	λ	NIST Special Pub 800-14	<p>The standard is currently being met partially. Previous year audits indicate that NSLDS needed to tighten up on some areas of auditing and monitoring (see red text below). Evidence made available does not indicate that these weaknesses have been addressed, nor was enough information provided to allow an assessment of the NSLDS audit and audit assessment posture. RACF is used to record auditable events, but the granularity of audit that can be achieved was not discussed, nor were procedures for reviewing audit records.</p> <p>No audit tool is available to monitor the SSN search activities.</p> <p>NSLDS audit review is not performed on a daily basis.</p>	Ensure NSLDS audit results are being used effectively to help NSLDS managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.

RFMS

[CBS](#)

[CPS](#)

[DLCD/DLSS](#)

[DLOS](#)

[FFEL](#)

[NSLDS](#)

[PEPS](#)

[TIVWAN](#)

RFMS Issue	Current Status	Standard	Observations	Opportunities for Improvement
General Description/Purpose	λ	NIST Special Pub 800-18	The standard is currently being met. Documented most recently in the RFMS ADP Systems Security Review, June 1998, and NIST 800-18 Questionnaire, 7/21/00.	Ensure complete and accurate descriptions, including detailed network and business process diagrams, are included in the Pell system security plan. See the Recommendations section for additional details.
Central Security Focus/Assigned Responsibility	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met partially.	Ensure the CBS SSO is properly trained and qualified. See the section on security training and awareness , and the related recommendations relating to the Promote Awareness phase of the risk management cycle. In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.
System Environment	λ	NIST Special Pub 800-18	The standard is currently being met.	See the recommendation for General Description/Purpose above.
System Interconnection/Information Sharing	λ	NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence that the interfaces had been addressed in the Security, Internal Controls, and Auditability Plan.	Ensure all Pell connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.
Applicable Laws and Regulations	λ	NIST Special Pub 800-18, Privacy Act, A-130 Appendix I	The RFMS has one published system of records, 18-40-0015, most recently updated in 1998. Privacy Act data includes name, address, birthdate, social security number, and financial data. Information is retrieved by social security number (SSN). A Privacy Act notice was published for this system, and was most recently updated in June 1998. No alterations have been made to the system of records. RFMS has implemented and documented policies and procedures for storage, retrieval, access, retention, and disposal of records in accordance with Privacy Act requirements. These policies and procedures were last updated in June 2000. RFMS does not participate in any matching program with any other agency.	N/A; Pell appears to be in compliance with Privacy Act requirements.

RFMS Issue	Current Status	Standard	Observations	Opportunities for Improvement
			<p>The contract with ACS requires contractors to comply with Privacy Act requirements.</p> <p>Training on security, including privacy act requirements, is provided to all Department of Education employees and contractors annually.</p> <p>Disclosures of Privacy Act information are made by telephone to participating schools in accordance with the system's published routine use. The date, time, and content of the phone calls are logged. Applicants are not given direct access to their data through this system, but may access their data through other databases maintained by SFA. Pell ensures that individual records are accurate through editing software, software testing, and SFA testing and review. Most employees have "read-only" access. Very few people have "read-write-modify" access to data.</p>	
Description of Information Sensitivity	λ	NIST Special Pub 800-18	The standard is currently being met.	See the Recommendations relating to developing a security model below.
Risk Assessment and Management	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Implement the GAO risk management cycle in the Pell environment. See the other improvement suggestions for this systems as well as the Conclusions and Recommendations sections.
Review of Security Controls	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Ensure future controls reviews measure the maturity of the Pell risk management cycle.
Rules of Behavior	λ	OMB A-130	The standard is currently being met.	Ensure managers and users are trained to understand them.
Security Life Cycle Planning	λ	NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>There was no evidence of appropriate security controls for the Maintenance, Disposal, and Authorization phases of the System Development Life Cycle.</p>	Ensure privacy and security in the information life cycle are addressed in Pell life cycle planning documents. See the Security Life Cycle Planning section for additional details.
Authorize Processing	λ	OMB A-130	<p>The standard is currently being met partially.</p> <p>Although Pell has not sought certification recently, this report could serve as the basis for a system certification/authority to operate.</p> <p>Prior to this security review, Pell had not been certified</p>	Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal Pell certification test under NIST guidance (FIPS 102).

RFMS Issue	Current Status	Standard	Observations	Opportunities for Improvement
			or granted approval to operate by a DAA within the last five years.	
Personnel Security	λ	OMB A-130	<p>The standard is currently being met partially.</p> <p>Incomplete security forms provided by ACS has caused delays in initiating the background screening for contract employees.</p> <p>Security is not specifically mentioned in key ED personnel position.</p> <p>ACS has received no official notification of the results of any of the background screenings.</p>	Implement ED personnel security guidance. See the Personnel Security section for additional details.
Physical and Environmental Protection	λ	NIST Special Pub 800-18	<p>The standard is currently being met.</p> <p>Pell benefits from the physical and environmental controls at the Meriden VDC.</p>	When developing/updating the Pell security plan, ensure the controls noted above are fully addressed.
Production, Input/Output Controls	λ	NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>References were made to documents that were not included with the document under review.</p> <p>Status of the production and input/output controls is unknown to the reviewers as the environment and contractors have changed since the last review.</p>	Implement Security Life Cycle Planning , Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the Pell security plan.
Contingency Planning	λ	OMB A-130	<p>The standard is currently being met partially.</p> <p>Continuity of operations planning (for users) and disaster recovery planning for portions of RFMS run at ACS are not complete. These plans need to address critical dependence on key staff as a potential point of failure.</p> <p>ED participated in the establishment of an incident response capability that made available the resources of the NASA Computer Incident Response Capability (NACIRC). This incident response capability was not funded and is no longer available.</p> <p>ACS controls and procedures for computer incident response are not formally documented.</p>	Ensure formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the Pell SSO has a copy of all plans.

RFMS Issue	Current Status	Standard	Observations	Opportunities for Improvement
Application Software Maintenance Controls	λ	NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>There was no evidence that procedures are in place to protect against illegal use of software.</p> <p>No separate test environment exists.</p> <p>Testing is not performed in a rigorous manner.</p> <p>Once PRC lost the follow-on contract, there was difficulty in getting PRC staff to meet contract requirements.</p> <p>The RFMS production and test environments are mixed.</p> <p>ACS used a unlock/rename/lock process to manage program changes.</p> <p>Lack of a true test environment is a concern.</p> <p>Production access can eliminate/bypass the librarian control.</p> <p>Undue reliance on a single individual for continued operation of the RFMS.</p> <p>Timely ED approval for production changes is a concern.</p> <p>Growing number of overrides pointing to libraries considered developmental.</p>	<p>Examine ED guidance relating to system life cycle planning. Ensure that Pell CM processes and procedures are consistent with that guidance, and that the Pell SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.</p>
Data Integrity/Validation Controls	λ	NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>Integrity and availability are the primary concerns for RFMS. Related to these concerns are members CDSPS01, CDSPS03, CDSPA17, CDSPA02, and CDSPA24. Those with “S” in the 5th position are the most unreliable and those with “A” in the 5th position can cause the most damage to RFMS.</p>	<p>Ensure Pell complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details.</p>
Documentation PGRFMS	λ	NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>The Security Plan does not meet the requirements of the Computer Security Act of 1987, and OMB 90-08.</p> <p>RFMS application documentation is not current and ACS staff are not at all satisfied with the system documentation that exists.</p>	<p>Develop a NIST-compliant (Special Pub 800-18) security plan for Pell. See the Recommendations section for additional details.</p>
Identification and	λ	NIST Special Pub 800-	<p>The standard is currently being met partially.</p>	<p>Ensure Pell complies with SFA standards for data user</p>

RFMS Issue	Current Status	Standard	Observations	Opportunities for Improvement
Authentication		14, NIST Special Pub 800-18	<p>No password dictionary checking is performed to prevent users from choosing easily-guessed passwords (common passwords).</p> <p>The amount of time it takes to receive a user ID after submission of the ITS form 88-01 seems longer than necessary.</p>	IDs and passwords. See the Identification and Authentication Section above for detailed guidance.
Logical Access Controls	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>Production programs are supposed to run from the production library, which is a protected library. Overrides have been requested to allow production programs to run from the development library.</p> <p>No other controls over dialing in, such as restricting incoming calls to those from modem pools or those with dial-back are used.</p> <p>Lockheed-Martin staff were directed by ED to maintain the existing rules that PRC created and have been following the previously-defined RACF rules.</p> <p>The lack of defined policies and procedures has increased the difficulty of day-to-day operations as well as routine tasks.</p>	Document and implement within one year Pell-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.
Public Access Controls	λ	OMB A-130	The standard is currently being met.	Document and implement within one year Pell-specific policies, standards, procedures and guidelines to govern public access processes and mechanisms.
Security Awareness and Training	λ	OMB A-130, NIST Special Pub 800-14	<p>The standard is currently being met partially.</p> <p>References were made to documents that were not included with the document under review.</p> <p>Security awareness and training are especially important given the maintenance and development environment.</p> <p>Contractors on-site at ED have not received any specific security training or refresher awareness briefings.</p> <p>The ED Functional System Manager has received no systems security training.</p> <p>There is not formal security awareness program with the RFMS, OPE, or SFA.</p> <p>RFMS management is satisfied with the level of security</p>	Provide security training for the Pell SSO; once trained, the Pell SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.

RFMS Issue	Current Status	Standard	Observations	Opportunities for Improvement
			awareness; however, they also stated that it could be improved.	
Audit Trails	λ	NIST Special Pub 800-14	<p>The standard is not currently being met.</p> <p>There was no evidence that procedures were in place to review audit trails.</p> <p>No ongoing effort to ensure there is a complete audit trail that records user activity.</p> <p>The “Protectall” feature of RACF is not activated. This would provide default protection for datasets and other general resources.</p> <p>Seven program names have the privilege to bypass RACF password authorization checking, per the DS-MON report.</p> <p>The RACF audit function is not used to track the activities of selected (privileged) users.</p>	Ensure Pell audit results are being used effectively to help Pell managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.

PEPS

[CBS](#)

[CPS](#)

[DLCD/DLSS](#)

[DLOS](#)

[FFEL](#)

[NSLDS](#)

[RFMS](#)

[TIVWAN](#)

PEPS Issue	Current Status	Standard	Observations	Opportunities for Improvement
General Description/Purpose	λ	NIST Special Pub 800-18	The standard is currently being met. Documented most recently in the PEPS OMB A-130 System Security Report, March 22, 1999.	Ensure complete and accurate descriptions, including detailed network and business process diagrams, are included in the PEPS system security plan. See the Recommendations section for additional details.
Central Security Focus/Assigned Responsibility	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met partially. Data ownership has not been defined clearly.	Ensure the CBS SSO is properly trained and qualified. See the section on security training and awareness , and the related recommendations for the Promote Awareness phase of the risk management cycle. In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.
System Environment	λ	NIST Special Pub 800-18	The standard is currently being met.	See the recommendation for General Description/Purpose above.
System Interconnection/Information Sharing	λ	NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of Memoranda of Understanding (MOU), or Trading Partner Agreements (TPA), or that the interfaces had been addressed in the Security Plan.	Ensure all PEPS connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.
Applicable Laws and Regulations	λ	NIST Special Pub 800-18, Privacy Act, A-130 Appendix I	PEPS is cognizant of applicable laws and regulations. The status of Privacy Act compliance is unknown. Although this system presumably complies with notice, publication, and annual/biennial/quadrennial review requirements, as those remain the responsibility of the Department's Chief Privacy Officer, no system-specific information with regard to access controls, storage, retrieval, retention, disclosure logging, contractor compliance, disposal of records, or employee training was provided for these systems.	N/A
Description of Information Sensitivity	λ	NIST Special Pub 800-18	The standard is currently being met.	See the Recommendations relating to developing a security model below.
Risk Assessment and Management	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Implement the GAO risk management cycle in the PEPS environment. See the other improvement suggestions for this systems as well as the Conclusions and

PEPS Issue	Current Status	Standard	Observations	Opportunities for Improvement
				Recommendations sections.
Review of Security Controls	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Ensure future controls reviews measure the maturity of the PEPS risk management cycle.
Rules of Behavior	λ	OMB A-130	The standard is currently being met.	Ensure managers and users are trained to understand PEPS rules of behavior.
Security Life Cycle Planning	λ	NIST Special Pub 800-18	The standard is not currently being met. There was no evidence of appropriate security controls for each phase of the System Development Life Cycle.	Ensure that (as appropriate) privacy and security in the information life cycle are addressed in PEPS life cycle planning documents. See the Security Life Cycle Planning section for additional details.
Authorize Processing	λ	OMB A-130	The standard is not currently being met. Although PEPS has not sought certification, this report could serve as the basis for a system certification/authority to operate.	Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal PEPS certification test under NIST guidance (FIPS 102).
Personnel Security	λ	OMB A-130	The standard is currently being met.	Implement ED personnel security guidance. See the Personnel Security section for additional details.
Physical and Environmental Protection	λ	NIST Special Pub 800-18	The standard is currently being met. PEPS benefits from the physical and environmental controls at the Meriden VDC.	When developing/updating the PEPS security plan, ensure the controls noted above are fully addressed.
Production, Input/Output Controls	λ	NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of controls for the installation and use of the application.	Implement Security Life Cycle Planning , Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the PEPS security plan.
Contingency Planning	λ	OMB A-130	The standard is currently being met.	Ensure formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the PEPS SSO has a copy of all plans.
Application Software Maintenance Controls	λ	NIST Special Pub 800-18	The standard is not currently being met. There was no evidence of controls for the maintenance of the application.	Examine ED guidance relating to system life cycle planning. Ensure that PEPS CM processes and procedures are consistent with that guidance, and that the PEPS SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.
Data Integrity/Validation	λ	NIST Special Pub 800-	The standard is not currently being met.	Ensure PEPS complies with SFA standards for data

PEPS Issue	Current Status	Standard	Observations	Opportunities for Improvement
Controls		18	There was no evidence of controls for assuring the integrity and validity of the data.	integrity and automated validations. See the Data Integrity section for additional details.
Documentation	λ	NIST Special Pub 800-18	The standard is currently being met.	Ensure the PEPS security plan is NIST -compliant.
Identification and Authentication	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>There was no evidence of policies for defining the password management process, or procedures for monitoring it.</p> <p>The minimum user password length for the Oracle and ReachOut systems is significantly shorter than the industry standard six-character.</p> <p>PEPS user initial passwords are defaulted to UserIDs, which are known to all PEPS users.</p> <p>Oracle and ReachOut systems allow trivial passwords.</p> <p>The Oracle, HP/UX, and ReachOut systems do not force the users to change their passwords periodically.</p> <p>The convention for assigning PEPS user initial passwords is stated in the PEPS System Security Plan.</p>	Ensure PEPS complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.
Logical Access Controls	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>There was no evidence of policies for defining the logical access control process, or procedures for monitoring it.</p> <p>Oracle users are given unlimited invalid logon attempts by rebooting their workstations.</p> <p>Terminated employee access or employees who no longer need access to PEPS aren't removed from system.</p>	Document and implement within one year PEPS-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.
Public Access Controls	λ	OMB A-130	The standard is currently being met.	Ensure PEPS-specific policies, standards, procedures and guidelines to govern public access processes and mechanisms are documented in the PEPS security plan.
Security Awareness and Training	λ	OMB A-130, NIST Special Pub 800-14	<p>The standard is not currently being met.</p> <p>There was no evidence of policies or procedures for implementing a security awareness program.</p> <p>Security awareness training has not been implemented for the school and GA user community.</p>	Provide security training for the PEPS SSO; once trained, the PEPS SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.

PEPS Issue	Current Status	Standard	Observations	Opportunities for Improvement
Audit Trails	λ	NIST Special Pub 800-14	The standard is currently being met partially. <i>Auditing on the HP/UX is disabled.</i> <i>Auditing on the Oracle RDBMS is disabled.</i>	Ensure PEPS audit results are being used effectively to help PEPS managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.

TIVWAN

[CBS](#)

[CPS](#)

[DLCD/DLSS](#)

[DLOS](#)

[FFEL](#)

[NSLDS](#)

[RFMS](#)

[PEPS](#)

TIVWAN Issue	Current Status	Standard	Observations	Opportunities for Improvement
General Description/Purpose	λ	NIST Special Pub 800-18	The standard is currently being met. Documented most recently in the TIVWAN ADP Systems Security Review, July 1997, and NIST 800-18 Questionnaire, 8/10/00.	Ensure complete and accurate descriptions, including detailed network and business process diagrams, are included in the TIVWAN system security plan. See the Recommendations section for additional details.
Central Security Focus/Assigned Responsibility	λ	OMB A-130, NIST Special Pub 800-14	The standard is currently being met partially. The ACSO is not appointed in writing. The ACSO has not attended an ACSO meeting regularly and the ACSO does not have an alternate to attend in his/her place. Conflicts have arisen over TIVWAN security controls and methods for implementation. Conflicts exist among TIVWAN, OPE, and TIVWAN applications management regarding what controls are required, who is responsible for implementing them, and how to best implement controls exist. Separation of duties for individuals with security responsibilities is achieved only partially. Security personnel lack adequate training in technology and IT security necessary to evaluate operational anomalies for security incidents or concerns.	Ensure the TIVWAN SSO is properly trained and qualified. See the section on security training and awareness , and the related recommendations for the Promote Awareness phase of the risk management cycle. In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.
System Environment	λ	NIST Special Pub 800-18	The standard is currently being met.	See the recommendation for General Description/Purpose above.
System Interconnection/Information Sharing	λ	NIST Special Pub 800-18	The standard is currently being met partially. There was no evidence of Memoranda of Understanding (MOU), or Trading Partner Agreements (TPA), or that the internal interfaces had been addressed in the Security Plan.	Ensure all TIVWAN connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.
Applicable Laws and Regulations	λ	NIST Special Pub 800-18, Privacy Act, A-130 Appendix I	TIVWAN is cognizant of applicable laws and regulations. The status of Privacy Act compliance is unknown. Although this system presumably complies with notice, publication, and annual/biennial/quadrennial	N/A

TIVWAN Issue	Current Status	Standard	Observations	Opportunities for Improvement
			review requirements, as those remain the responsibility of the Department's Chief Privacy Officer, no system-specific information with regard to access controls, storage, retrieval, retention, disclosure logging, contractor compliance, disposal of records, or employee training was provided for these systems.	
Description of Information Sensitivity	λ	NIST Special Pub 800-18	The standard is currently being met.	See the Recommendations relating to developing a security model below.
Risk Assessment and Management	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Implement the GAO risk management cycle in the TIVWAN environment. See the other improvement suggestions for this system as well as the Conclusions and Recommendations sections.
Review of Security Controls	λ	OMB A-130	This risk assessment serves to satisfy the standard.	Ensure future controls reviews measure the maturity of the TIVWAN risk management cycle.
Rules of Behavior	λ	OMB A-130	The standard is currently being met partially. Rules of behavior have not been documented specifically.	Document rules of behavior for TIVWAN. Ensure managers and users are trained to understand them.
Security Life Cycle Planning	λ	NIST Special Pub 800-18	The standard is not currently being met. There was no evidence of appropriate security controls for the Maintenance, Disposal, and Authorization phases of the System Development Life Cycle.	Ensure that (as appropriate) privacy and security in the information life cycle are addressed in TIVWAN life cycle planning documents. See the Security Life Cycle Planning section for additional details.
Authorize Processing	λ	OMB A-130	The standard is not currently being met. Although TIVWAN has not sought certification, this report could serve as the basis for a system certification/authority to operate.	Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal TIVWAN certification test under NIST guidance (FIPS 102).
Personnel Security	λ	OMB A-130	The standard is currently being met partially. Security is not mentioned specifically in key ED and NCS personnel position descriptions. No specific procedures have been established for updates to personnel clearances/background investigations. No access termination statements have been established for departing or transferred NCS employees to certify their awareness of their continuing responsibility to safeguard data subject to the Privacy Act.	Implement ED personnel security guidance. See the Personnel Security section for additional details.

TIVWAN Issue	Current Status	Standard	Observations	Opportunities for Improvement
			<p>No clarification as to whether or not the TIVWAN ACSO should be checking the SSN of the users against the NSLDS database to verify if the user is in default on a student loan.</p> <p>306 forms are not stored in a secured area.</p> <p>GEIS staff are not provided feedback as to when they are cleared and at what level.</p>	
Physical and Environmental Protection	λ	NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>The newly-designed regular employees' badges will not have an expiration date.</p> <p>The tape library is not separated by a firewall from the clean room, which poses additional risk.</p> <p>The section of the TIVWAN Security Plan that covers the physical security measures of GEIS does not provide specifics. The plan is also generalized and contains statements that need further clarifications.</p>	When developing/updating the TIVWAN security plan, ensure the controls noted above are fully addressed.
Production, Input/Output Controls	λ	NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>The destination point file is provided nightly from NCS to NSLDS, but NSLDS is using paper documents instead. Changes to information on the forms by NCS staff should not be happening.</p> <p>Inappropriate information has been sent to schools. Documents reviewed showed changes, without any initials or names to provide accountability for who had made the changes. This is contrary to NCS procedures.</p> <p>Data is misdirected as a result of human error. This error has been compounded by a failure to follow established procedures, thereby eliminating the audit trail.</p>	Implement Security Life Cycle Planning , Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the TIVWAN security plan.
Contingency Planning	λ	OMB A-130	<p>The standard is currently being met partially.</p> <p>The Contingency Planning section of the Security Plan is potentially out-of-date and lacks documentation of detailed procedures. The emergency response operations sections are high-level.</p> <p>Copies of the plan are maintained in machine-readable</p>	Ensure formal contingency and incident response plans are consistent with NIST guidance (Special Pub 800-3). Ensure plans are exercised once annually, and the TIVWAN SSO has a copy of all plans.

TIVWAN Issue	Current Status	Standard	Observations	Opportunities for Improvement
			(electronic) format at the off-site facility. Key personnel do not maintain printed copies of the plan at their homes.	
Application Software Maintenance Controls	λ	NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>There was no evidence that controls were in place to protect against the illegal use of software.</p> <p>The Configuration Manager's training in CM has not included the full scope and responsibilities of a CM program.</p> <p>The end-user software does not indicate the last time and date of access to help them determine if anyone other than themselves has used the software.</p> <p>Programmers have had no training specific to IT security. Thus, it would be unlikely that they can identify vulnerabilities when making changes to software.</p> <p>Developers are allowed to move their own code from the test environment to the production environment using JCL statement. If any part of the JCL statement is missing (from using "cut & paste" method), it could mean that the test program could be run against the production database. If the test program changed many records, the repair could be costly.</p> <p>Developers, administrators, and systems analysts have access, update, and delete authority in all three databases used for TIVWAN (two test databases and one production database). Any member of the development group could create a program and bind it to the production database.</p> <p>NCS technical staff is not notified by GEIS prior to GEIS staff taking the system down for maintenance.</p> <p>It is unlikely that the institutions supported by TIVWAN are Y2K compliant, which could cause a failure in TIVWAN.</p>	Examine ED guidance relating to system life cycle planning. Ensure that TIVWAN CM processes and procedures are consistent with that guidance, and that the TIVWAN SSO is integrated into the systems development and CM processes. SSO should be part of the approval chain for all proposed changes to system software.

TIVWAN Issue	Current Status	Standard	Observations	Opportunities for Improvement
Data Integrity/Validation Controls	λ	NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>Security on mainframes – manufacturers of mainframes, such as IBM, provide a system integrity statement that defines their acceptance of responsibility for system integrity and describes the system changes that transfer that responsibility to the user.</p> <p>In the current PC/LAN environment, it is incumbent upon the user to establish and maintain effective system integrity controls.</p> <p>The TIV WAN environment is comprised of mainframes and PC/LAN components. Thus, its integrity controls must cover both environments. NCS has focused its mainframe system where controls are well-established, unintentionally overlooking the PC/LAN where threats and vulnerabilities are greater.</p>	Ensure TIVWAN complies with SFA standards for data integrity and automated validations. See the Data Integrity section for additional details.
Documentation	λ	NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>The Security Plan was not included for review.</p> <p>The computer Security Plan for TIVWAN was a one-time deliverable without a version number.</p> <p>The TIVWAN Security Plan does not meet the requirements of the Computer Security Act of 1987 and OMB Bulletin 90-08.</p>	Develop a NIST-compliant (Special Pub 800-18) security plan for TIVWAN. See the Recommendations section for additional details.
Identification and Authentication	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>TIVWAN TG numbers are assigned to an institution. NSLDS assigns UserIDs to specific individuals. This creates a conflict between the TIVWAN and the NSLDS security procedures. TIVWAN performs no mapping or verification check between TIVWAN ID and NSLDS ID.</p> <p>Password dictionary checking is not performed to prevent users from choosing easily-guessed passwords (common passwords).</p> <p>Password resets are disproportionately high (300 per week for a community of 7,000 users).</p> <p>The Personal Identification Number (PIN) assignment, at the destination level, has yet to be implemented</p>	Ensure TIVWAN complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.

TIVWAN Issue	Current Status	Standard	Observations	Opportunities for Improvement
			<p>because of a lack of direction from the Government regarding its use. The PIN approach was developed as a cost-saving mechanism because of the volume of password resets required by customers. Implementation details yet to be resolved include how to provide the PIN to the individual.</p> <p>The Mark III system presents a vulnerability in that there are two times during the password change process when the passwords are stored as clear text (password change data are not compressed – only data are compressed). The first is when changing a password, the user submits the UserID, the old password, and the new password. A built-in password change procedure script signs the user onto the Mark III. The passwords are unencrypted until provided to Mark III, where they are encrypted for storage. The other is when the passwords are transferred to RACF, which is done in clear text, and then encrypted in RACF for storage.</p> <p>The password associated with the TG5 number can be changed easily. Individuals may call customer service or they may dial an automated voice response unit, enter their Z number and their TG5 number, and have their passwords reset. No additional information is required to provide assurance that the individual assigned to the TG5 number is the one changing the password.</p> <p>The one-to-one ratio of TIVWAN UserIDs to mailboxes does not appear to fit structure needed by institutions.</p>	
Logical Access Controls	λ	NIST Special Pub 800-14, NIST Special Pub 800-18	<p>The standard is currently being met partially.</p> <p>Reassigning of UserIDs: TIVWAN's position is that the schools or the institutions own the UserIDs, not the official at the school to whom the ID is assigned or the various individuals who use the ID (listed at technical contact points). Schools are allowed to change technical contact points. NSLDS management has taken the view that the UserID is owned by the individual, not the institution. On April 25, 1997, a decision was reached that NSLDS would allow the contact point to be changed. Details of this decision were not yet available.</p>	Document and implement within one year TIVWAN-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.

TIVWAN Issue	Current Status	Standard	Observations	Opportunities for Improvement
			<p>When multiple UserIDs are assigned to one customer, they are assigned sequentially. Potentially, by using the IVR to reset a password, a user could make an error entering their customer ID and accidentally reset another user's password.</p> <p>Per NSLDS, NCS staff was putting incorrect TG5 numbers on the PA form. The basic reason for the incorrect information appears to be the failure to follow established procedures and poor quality control.</p> <p>NCS is accepting forms and assigning TG5 numbers to applicants who are not following the requirements for providing valid SSNs and DOBs.</p> <p>A recent concern within NSLDS is that UserIDs may not be switched from one person to another. TIVWAN is allowing this, so they switch to a new person, send E-Systems the LOA, and the NSLDS software rejects the application. The LOAs are on hold because there are no directions from the Government. NSLDS may allow the switch, but if they do, special action and recordkeeping will be required to maintain appropriate audit trails.</p> <p>E-Systems has started receiving the electronic destination point file. They are in the testing phase. Thus far, NSLDS has been unwilling to accept the file 100 percent with information as input - first they want to do comparison and reject non-matches. There is no estimated completion date for this comparison.</p> <p>If the Destination file was sent twice in one night, this would be noticed and addressed, although there are no official procedures that specify the number of files allowed to be sent/received per night.</p>	
Public Access Controls	λ	OMB A-130	The standard is currently being met.	Document and implement within one year TIVWAN-specific policies, standards, procedures and guidelines to govern public access processes and mechanisms.
Security Awareness and Training	λ	OMB A-130, NIST Special Pub 800-14	<p>The standard is currently being met partially.</p> <p>The Functional Manager has had no systems security training.</p> <p>NCS does not have a security awareness or training</p>	Provide security training for the TIVWAN SSO; once trained, the TIVWAN SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.

TIVWAN Issue	Current Status	Standard	Observations	Opportunities for Improvement
			<p>program and no employees were identified as holding professional security certifications.</p> <p>Security issues are not given more attention. There is a perception at NCS that prosecutions for violations of the Privacy Act do not occur.</p>	<p>Recommendations sections for detailed guidance.</p>
<p>Audit Trails</p>	<p>λ</p>	<p>NIST Special Pub 800-14</p>	<p>The standard is currently being met partially.</p> <p>Security-specific analysis has not been performed on the audit trail data.</p> <p>Audit trails are not created at the application level. There are no reports of specific commands.</p> <p>The RACF audit function is not used to track the activities of selected (privileged) users.</p> <p>The Help Desk did not always verify that the caller was an authorized user by consistently checking to see if the caller is listed as the point of contact for the TG5 number.</p>	<p>Ensure TIVWAN audit results are being used effectively to help TIVWAN managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.</p>

Conclusions

SFA's enterprise-level risk management cycle is under-developed, and this immaturity is manifested at the system level.

While each individual system has its own unique opportunities for improvement, all are consistent in the areas where improvements can be made. In addition, areas that need to be improved are consistent over time—the same problems continue to be found in A-130 reviews and privacy/security assessments dating back over three years. This consistency leads us to conclude that system-level problems are merely symptomatic - reflections of weaknesses at the enterprise level. It also leads us to reason that improvements to enterprise-wide risk management processes will yield long-term benefits at the system level.

Implementing effective risk management at SFA will require improvements to every phase of the risk management cycle at the enterprise level. While each system should continue to pursue resolution of system-specific findings, we conclude that system-level risk management will be greatly facilitated and enabled by enterprise-wide risk management. Strengthening SFA's executive management ability to execute the four phases of the risk cycle will help to achieve economies of scale by reducing duplicative efforts at the system level. In addition, by establishing an SFA-wide risk management structure, system-level risk management will tend to be more consistent, leading to more predictable outcomes and more efficient allocation of resources.

Risk management is not about compliance with OMB and NIST guidance, it is about enabling SFA systems to more effectively support SFA's public service mission. Implementing effective risk management will require a consistent effort over time and a commensurate allocation of sufficient resources. However, over time the benefits of effective risk management can far outweigh the costs. These savings can be realized from prevention or early detection of a single risk event. Information and systems risk equates to business risk; risk management is good business.

Recommendations

Our principal recommendation is that SFA adopt the GAO risk management cycle. In support of this effort, we further recommend SFA perform activities to implement key risk management activities at the system level, with oversight and support from the Director and OCIO level. Displayed in the table below are discrete activities that we recommend SFA fund and perform. These recommendations are organized to illustrate which part of the risk management cycle they are intended to support, numbered in priority order, and based on the enterprise-wide and system-level opportunities for improvement articulated above.

Risk Management Cycle Stage	Issue Area	Recommendation	Priority
Assess Risks and Determine Needs	Functional and technical system descriptions	Develop detailed functional and technical descriptions for all systems, and provide as a common resource for use in all documentation.	5
	Security model	Develop a formal, SFA-wide security model.	11
	Risk assessment	Assess risk based on the GAO risk management model.	10
	Certification and Accreditation (C&A)	Certify and accredit all systems based on Federal Information Processing Standard (FIPS) 102.	12
Implement Policies and Controls	Security plans	Update or develop security plans for all systems.	2
	Security standards	Establish SFA-wide privacy and security standards, and ensure standards are reflected in system security plans.	6
	Rules of behavior	Develop rules of behavior that are consistent across all systems.	3
Promote Awareness	System Security Officer training	Provide security training for SSOs.	1
	Enterprise-wide security training and awareness	Develop and implement an enterprise-wide security training and awareness program.	4
Monitor and Evaluate	Metrics	Identify/develop metrics for measuring high-risk events. For all measurable events, establish clipping levels – the level of normally-expected high-risk events.	7
	Measurement	Use existing system audit tools to capture high-risk events.	8
	Feedback	Ensure the results of measurement activities are assessed at the individual system <i>and</i> enterprise level.	9

While SFA may choose to take steps to implement the GAO risk management model in any order it chooses, the ordering of the recommendations above is designed to ensure activities and processes that enable higher risk management functions are performed first. Taken out of order, some measures will be difficult to implement, and this may undercut support for taking further measures to establish a robust, business-oriented risk management cycle

Recommendation ordering is reasoned as follows:

1. The most pressing need is to improve the security skill sets of the personnel given responsibility for system security, the SSOs. Any other activities performed without this are not likely to succeed, or be implemented in an effective or efficient manner.
2. The next recommended activity, developing security plans, should be carried out by the SSOs in order to ensure they understand the security requirements for their systems and become familiar with Federal security requirements.
3. Rules of behavior are a NIST-based security plan requirement; the SFA CSO should provide oversight to ensure there is basic consistency across all systems.
4. Similarly, functional and technical descriptions should be developed as part of system security plans.
5. At this point the SFA CSO will have a sufficiently trained staff to develop and execute an enterprise-wide security training and awareness program. Training is one of the most cost-effective security controls available. For this reason, the SFA CSO should not delay in implementing this recommendation for any longer than is required to establish the skills and rules of behavior baseline the training is designed to inculcate.
6. Some standards will be developed in consultation with system owners and articulated in system security plans, but at some point entity-wide standards should be negotiated and established as the basis for future systems development and modification. As standards are developed and implemented, changes can be incorporated in training, rules of behavior, and security plans.
7. Other follow-on activities enabled by standards development are those associated with monitoring and evaluation. As standards are developed, so should metrics for high-risk events. A 'yardstick' for measuring system security performance should be developed for each system; some metrics will be common to all systems, others will be unique to particular system/business processes.
8. Once detailed standards and metrics are established, audit logs and other monitoring tools must be turned on to capture information on high-risk events. Where the technical capability falls short, other mitigating measures may be required.
9. Capturing audit events is pointless unless the information is subjected to analysis. SSOs should perform assessments monthly and report results to the SFA CSO. In addition, once analytical mechanisms have matured, the SFA CSO, in coordination with SSOs and system contractors, should develop and implement incident response procedures that are consistent across all systems.
10. At this point a sufficient number of controls and processes should be in place to make follow-on risk assessment worthwhile.
11. Developing a security model is a complex, long-term activity. The process of categorizing information, assigning a sensitivity level to each category, and assigning information ownership needs to be carried out with deliberation. A security model that is not well thought-out or improperly implemented can prove cumbersome and cost-inefficient.
12. Certification and accreditation is another long-term activity that must be set up properly to prove worthwhile. SFA should get the rest of its risk management activities implemented and normalized before attempting a full system certification and accreditation under FIPS 102 guidance. Until that time, periodic risk assessment may be used as the basis for issuing interim authority to operate.