



# **Student Financial Assistance eCampus Based System**

## **Risk Assessment Report**

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

Prepared by:



**November 4, 2001**

# TABLE OF CONTENTS

**EXECUTIVE SUMMARY ..... 2**

    BACKGROUND & METHODOLOGY ..... 2

    FINDINGS ..... 2

**BACKGROUND ..... 5**

    TASK OVERVIEW AND SCOPE ..... 5

    SYSTEM OVERVIEW ..... 6

    RISK ASSESSMENT BACKGROUND ..... 9

**CONCLUSIONS ..... 9**

Deleted: 55

# Executive Summary

## Background & Methodology

KPMG Consulting evaluated the risks inherent in the eCampus Based project supporting the Office of Student Financial Assistance's (SFA) core business process. To accomplish this task, KPMG Consulting security analysts attempted to collect information on eCampus Based's systems, network architectures, operations, physical environment where hardware is located, data elements and business processes. The approach used to gathered this information included inquiries to SFA Modernization Partner management and staff, and a thorough documentation review of eCampus Based's system security plan and initial business case. The available information was then analyzed to evaluate the maturity of eCampus Based's risk management model and to determine how well that model was being applied at the system level for the eCampus Based 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, 800-18, and 800-30. This measurement guidance was developed based on the Privacy Act of 1974 and the Computer Security Act of 1987.

## Findings

First and foremost, it is important to note that eCampus Based is a developing system. Therefore, the findings from this risk assessment should be incorporated into the life cycle development of the eCB system. Also, the data the eCB system maintains and transmits is not impacted by the privacy act, nor does it contain national security information. Moreover, eCB does not disburse student aid funds; rather, eCB plays a major role in the allocation of funds. Due to the nature of eCB data, any exploitation will have a very low impact to SFA as a whole, regardless of how likely the threat may occur. For this system, the likelihood of a threat occurring has also been minimized by the existing/planned system security controls, creating an overall risk level of low.

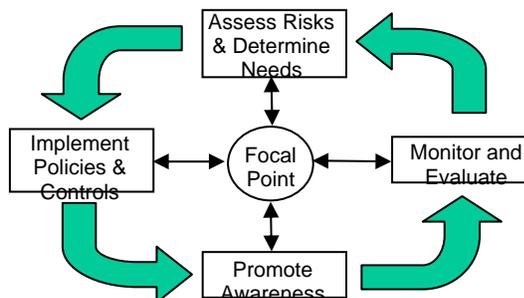


Figure 1: GAO Risk Management Cycle

The risks identified within eCB are mostly administrative in nature, and should be fairly easy to incorporate in the near future. This is important, because as eCB moves to full operational capability, it will be vital to have a solid procedural foundation to support any additional risks arising from new system functionality. We recommend the following actions, in priority order:

1. Pursue initial Certification and Accreditation and receive an interim approval to operate (IATO).
2. Incorporate SFA's Security Life Cycle checklists into the continuous development of eCB.
3. Obtain and review the contingency plan and disaster recovery plan maintained by the VDC. eCB should ensure its business process will be restored at the VDC if a contingency or disaster occurs.

4. Request and review the physical and environmental documentation from the Virtual Data Center. Include findings in the eCB system security plan.
5. Address the multiple findings in the Personnel Security portion of this assessment, including separation of duties procedures, termination procedures for a friendly and unfriendly termination, and explain the policy describing user access prior to a background investigation's completion.
6. Incorporate the numerous logical access control findings into the eCB security plan.
7. Increase the granularity of the eCB Input/Output documentation in the eCB security plan. This area should have detailed controls addressing specific Input/Output security measures.
8. Ensure compliance with all federal and departmental policies and guidelines explicitly noted in the eCB system security plan.

# Background

The eCampus-Based System (eCB System) enables the United States Department of Education (ED) to provide more than \$2 billion in Title IV student financial assistance funds to about 4000 post-secondary institutions each year through a complex allocation model. The system provides allocations/authorizations for grant, work-study, and loan funds to these institutions, and the institutions in turn use these funds to provide student financial assistance to more than 1,000,000 needy students each year. There are several distinct programs, each with its own legislative history and regulations, within the Campus-Based Programs. These include the Federal Supplemental Educational Opportunity Grant Program (FSEOG), Federal Work-Study Program (FWS), and Federal Perkins Loan Program (Perkins). The FSEOG program is for students with “exceptional” need (i.e. a sub-set of a school’s most needy Federal Pell Grant recipients.)

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 series 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*, NIST Special Pub 800-18, *Guide for Developing Security Plans for Information Technology Systems*, and NIST Special Pub 800-30, *Risk Management Guide*.

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 and scope**

KPMG Consulting performed a risk assessment of the proposed eCB system that will eventually be used by SFA to replace the legacy Campus Based System. This project was developed as a major application designed to support SFA’s business processes. Our goal was to assess the inherent risks of the eCB system, evaluating how security controls could be improved in order to help protect the system from threats it could face upon entering production.

KPMG Consulting employed several methods for obtaining information. This included a review of system documentation, recommendations for and a review of suggested procedural documentation, and briefings by Modernization Partner developers. This assessment did not include any physical testing or inspection of equipment.

The system boundaries used for this assessment encompass the eCB application housed at the Virtual Data Center in Meriden, CT. The security capabilities of the VDC themselves were not reviewed, as their practices will be held to their respective Service Level Agreements (SLAs) and contracts with SFA.

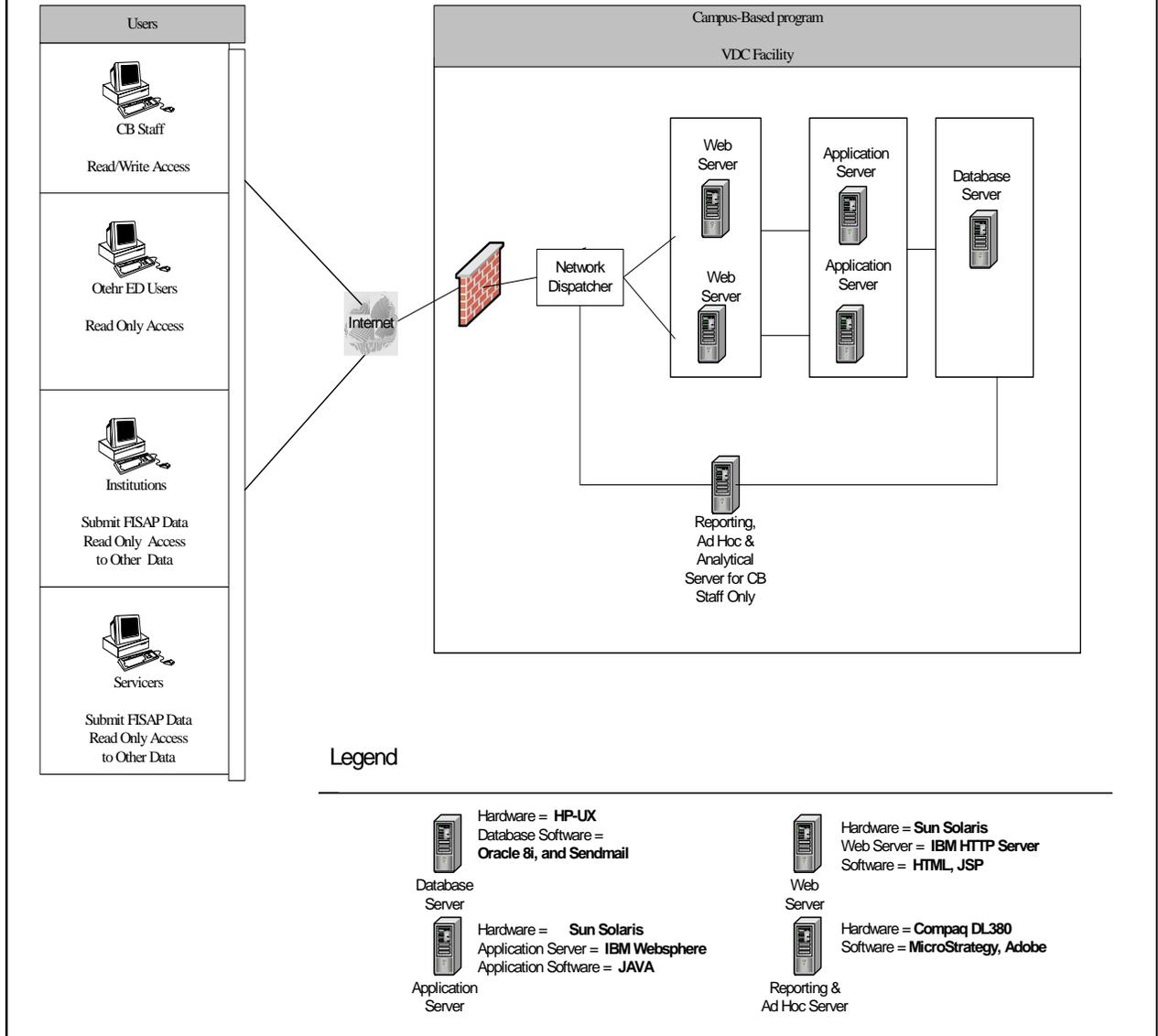
### ***System overview***

This initiative is designed to reduce cycle time for application processing for institutions, reduce risk from aging system, increase SFA staff access to data and analysis capabilities, provide institutions and servicers with an alternative submission option for the FISAP file and increase maintainability. It will effectively bring the CB application into today's technology, realizing the vision of the SFA Modernization, by moving it off of the mainframe scheduled for retirement, and provide efficient interaction with other relational database systems (FMS, COD, etc).

The physical servers that will be required for the redesigned eCB System are located in the list and following diagram:

- 2 Sun E3500 Web Servers using the Solaris Operating System
- 2 Sun E3500 Application Servers using the Solaris Operating System
- 1 Hewlett Packard 9000 V Class Database Server
- 1 Compaq DL380 Server

## Technical Architecture for Campus Based System



### Sensitivity/Criticality

All applications/systems require protection for confidentiality, integrity, and availability. The level of protection required is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the application/system to the organization's mission, and the economic value of the application/system components. The sensitivity and criticality of the information stored, processed by, or transmitted by the application/system provides a basis for the value of the application/system and is one of the major factors in risk management. A description of the types of information handled by the application/system and an analysis of the criticality of the information is required. This description and analysis will assist in designing security controls, facilitating security audits, and implementing security countermeasures.

eCB handles data related to the completion and submission of the FISAP. There is a need to protect the private financial information of schools, but there is no personal information of a Privacy Act nature (Social Security numbers etc.) needing protection.

The types of sensitive information the application/system accesses are limited to the data schools enter into the FISAP. Such data has administrative, financial, and grant/contract elements. Much of the information processed by the eCB system falls into the “integrity category” of basic protection requirements. This means that the information must be protected from unauthorized, unanticipated, or unintentional modification. Data that is classified under the “availability category” refers to information or services that must be available on a timely basis to meet mission requirements. There is no data handled by the eCB System that falls into the “Confidentiality Category.” In terms of sensitivity, most of the data handled by the eCB system is considered to be either of Low or Medium Sensitivity.

**APPLICATION/SYSTEM PROTECTION REQUIREMENTS CHART**

<b>Application/System Protection Requirements</b>	<b>High</b>	<b>Medium</b>	<b>Low</b>
Confidentiality			X
Integrity		X	
Availability			X

Estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the application/system would be that schools could have inadequate amounts of funding provided.

**APPLICATION/SYSTEM PROTECTION REQUIREMENTS CHART**

<b>Information Type</b>	<b>Confidentiality (High, Medium or Low)</b>	<b>Integrity</b>	<b>Availability</b>
Administrative		X	
Financial		X	
Grant/Contract		X	

There are two periods of time to consider when assessing the risk and impact of a system outage for the eCB system. During the time between 9/15/2001 through 12/31/2001 will have a parallel operational mode occurring where the legacy CB system will operate in conjunction with the eCB system. During this time period, if the eCB system suffers from an outage the users of the system will be able to enter their pertinent information into the current legacy CB system. This should minimize the potential impact of an eCB system outage. Second, after 12/31/2001, an eCB system outage will have a negative impact in terms of the users data entry schedule. Only extended outages of a couple of weeks or more would have the potential of disrupting institutional awards due to the extended period of time that the user has allocated in order to enter the FISAP information.

## **Risk Assessment Background**

We used GAO's Risk Management Cycle and NIST Special Pub 800-30 as the standards 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," and per NIST 800-30 created the threat-source/vulnerability pairs for each control area. A-130 Appendix I, A-130 Appendix III and security guidance contained in NIST Special Pub 800-12 and Special Pub 800-18 provided the specific standards against which we could measure SFA system compliance.

During our assessment, we examined the level of compliance in each issue/control area, taking into account the business process supported by eCB. A "stop light" grade was assigned to each issue/control area. 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 system level risk management. *For this reason there are a number of instances where opportunities for improvement are provided at the system level for control areas that have been given a green stoplight.*

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 and NIST guidance, and to provide useful, cost-effective recommendations for improving risk management processes. A diagram of a mature risk management model follows, with links to the control areas analyzed in this assessment.

# Overview of SFA System Risk Management Maturity

- [General Description/Purpose](#)
- [System Environment](#)
- [System Interconnection/Information Sharing](#)
- [Applicable Laws or Regulations](#)
- [General Description of Information Sensitivity](#)
- [Risk Assessment and Management](#)
- [Review of Security Controls](#)

- [Rules of Behavior](#)
- [Security life cycle planning](#)
- [Authorize Processing](#)
- [Personnel Security](#)
- [Physical and Environmental Protection](#)
- [Production, Input/Output Controls](#)
- [Contingency Planning](#)
- [Application Software Maintenance Controls](#)
- [Data Integrity/Validation Controls](#)
- [Documentation](#)
- [Identification and Authentication](#)
- [Logical Access Controls](#)
- [Public Access Controls](#)

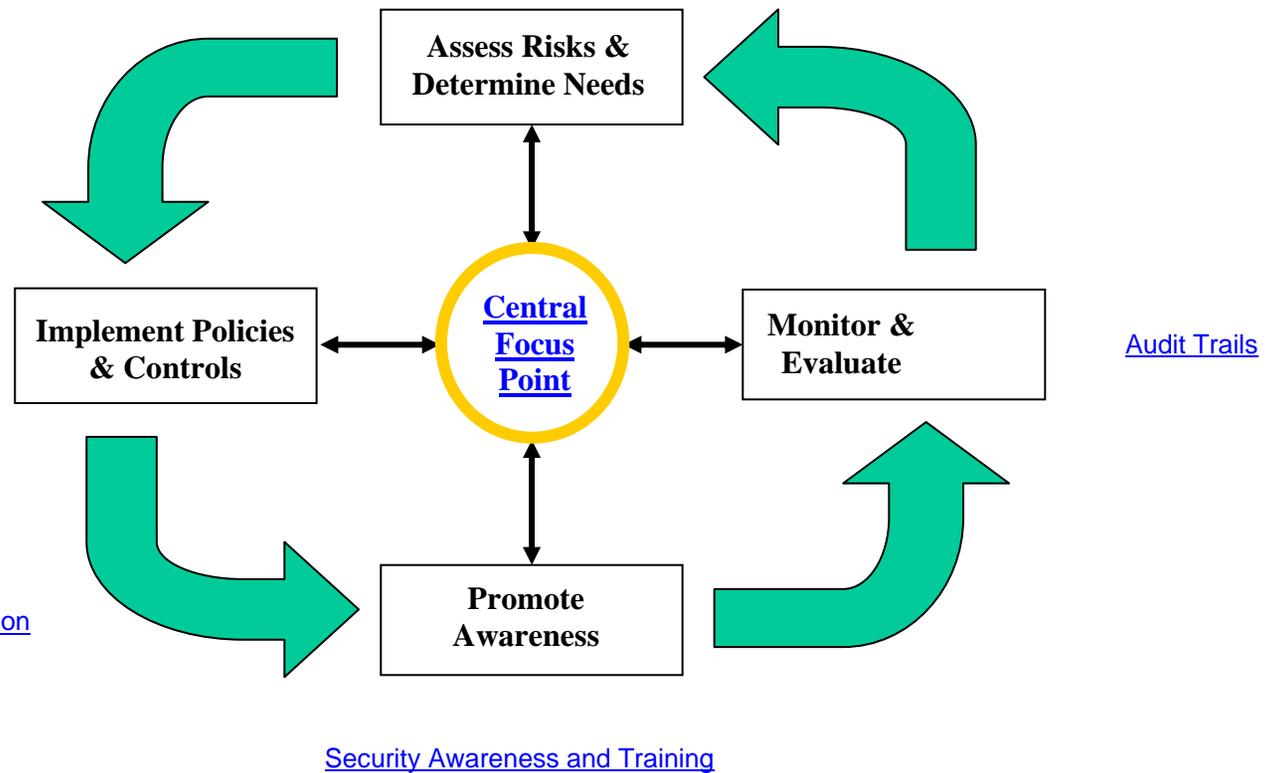


Figure 1: SFA System Risk Management Maturity Overview

Green

## Central Security Focus/Assigned Security Responsibility

[Back to Risk Cycle Illustration](#)

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

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

- 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

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.

### Significance in the SFA Environment:

**Threat:** Ambiguity in security policies, procedures, or management roles, leading to insecure practices with a lack of overall responsibility.

**Impact:** 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 SFA managers and security officers do not have adequate security backgrounds; in the near term only training can provide them with the needed knowledge baseline. The best source for that training comes from learning the underlying security policies and procedures of a given system.

### **Current Status:**

Currently, SFA is in the midst of improving its security policies and procedures. SFA has a set of security policies currently in review that will be distributed upon finalization. ECB should review the policies once finalized to ensure compliance with SFA requirements.

ECB has assigned an SSO for the system. Although verbally confirmed, no evidence of an SSO designation letter existed in the review material. Also, the SSO position was recently shifted to a new SFA person. The new SSO should request and receive proper training as soon as possible

### **Opportunities for Improvement:**

SFA needs to continue documenting their policies and procedures so as to provide a complete framework with which to manage risks. The system owner should designate the SSO assignment in writing, and the assignment letter should be included in the system security plan.

Green

## General Description/Purpose

[Back to Risk Cycle Illustration](#)

### 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).

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.

### Significance in the SFA Environment:

**Threat:** An unclear system description/purpose leads to "system creep", inaccurate system boundaries, and offers no foundation from which to assess threats to the organizational mission.

**Impact:** Accurate, complete system descriptions in system security plans provide several long-term benefits. 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.

### Current Status:

An accurate general description and purpose has been created for the eCB system. This description is paraphrased in most documentation, providing consistency throughout the system. The eCB security plan describes numerous components of the system boundary, such as interconnections and mission objective, but does not organize the information into a system boundary section. Ideally, the eCB security plan would describe a logical and physical diagram of the system, the interconnections with other sections, any pertinent operating characteristics, and the overall mission objective.

### **Opportunities for Improvement:**

Ensure the continued consistent use of established general descriptions and purpose passages for all future documentation. Update the description as eCB progress through its development.

**Green**

## System Environment

[Back to Risk Cycle Illustration](#)

### Standard: **NIST Special Pub 800-18**

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.)

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

Include any security software protecting the system and information.

### Significance in the SFA Environment:

**Threat:** Unclear system descriptions hamper system reconstruction during disaster recovery, incomplete software patches or hardware maintenance, and imperfect system security coverage.

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

### Current Status:

General descriptions of the system's technical architecture and make-up are available and in good order. Detailed network architecture diagrams, including manufacturers and model numbers of equipment, are documented. A compiled list of system hardware, software, and communications resources is currently available in the eCB Security plan.

### Opportunities for Improvement:

Ensure that network architecture diagrams are kept up-to-date with as much detail included as possible. Also, make sure the system security plan is kept up-to-date with any changes in software versions or hardware modifications. Maintain the complete list of hardware, software and communications in the security plan as the system progresses through its lifecycle.

Green

## System Interconnection/Information Sharing

[Back to Risk Cycle Illustration](#)

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

OMB Circular A-130 requires that written management authorization (often in the form of a Memorandum of Understanding or Service Level Agreement,) be obtained prior to connecting with other systems and/or sharing sensitive data/information. It is required that written authorization (MOUs, SLAs) 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.

### Significance in the SFA Environment:

**Threat:** Vague rules within the MOUs or SLAs create loopholes in which security requirements can be unintentionally relaxed without notice or legal ramifications, potentially causing harm to the system.

**Impact:** Formal MOUs or SLAs 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 control. If the business process it supports can define a system's boundaries, 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.

For eCB, strong SLAs are not required as a component of the system's documentation according to SFA policy. eCB only connects with other SFA systems, and as a result, is not required to establish service level agreements.

### Current Status:

The eCB security plan identifies three SFA systems with connections to eCB: CPS Mainframe, Pell Mainframe/Campus Based NT Server, and TIVWAN. The eCB business case mentions eventual connections with FMS and COD. These connections represent the critical business functions eCB will attempt to deliver, and as a result, should be documented in as much detail as possible.

### **Opportunities for Improvement:**

Since eCB relies on other SFA systems and facilities, the security plan should maintain all relevant documentation from the interconnected systems security plans. At a minimum, the eCB SSO should reference the interconnected systems security plans, including appropriate version and section numbers containing the applicable information (especially COD and FMS).

Also, TIVWAN is being replaced by the SFA to the Internet initiative. When this evolution is complete, eCB should update its interconnection list appropriately.

**Yellow**

## Applicable Laws and Regulations

[Back to Risk Cycle Illustration](#)

### 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:

**Threat:** Not knowing which laws are applicable makes it difficult to self-assess a system's compliance and ensure adequate measures have been taken to protect information.

**Impact:** 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:

eCB does not maintain privacy act data, but does interface with systems that do operate with Privacy Act data. Also, eCB does have operating requirements that could be impacted by loss of data integrity and system availability and should take special precaution to ensure all applicable expert insight is incorporated into eCB.

#### Opportunities for Improvement:

The eCB security plan references several applicable federal guidelines and regulations. While not required, the eCB security plan should indicate how the system or its personnel complies with each of the statements. A brief statement addressing this issue would enhance the viability of the security plan and ensure compliance with all regulations the eCB team "signed-up" to in the security plan.

**Green**

## Description of Information Sensitivity

[Back to Risk Cycle Illustration](#)

### Standard: NIST Special Pub 800-18

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**.

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.

### Significance in the SFA Environment:

**Threat:** Misappropriation of security assets and funding may be assigned to low-ranking threats while higher ranking requirements are under-protected or neglected.

**Impact:** 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.

### Current Status:

The system handles data related to the completion and submission of the FISAP. There is a need to protect the private financial information of schools, but there is no personal information of a Privacy Act nature (Social Security numbers etc.) needing protection. The type of sensitive information the application/system accesses is limited to the data schools enter into the FISAP, such data has administrative, financial, and grant/contract elements.

Much of the information processed by the eCB system falls into the “integrity category” of basic protection requirements. This means that the information must be protected from unauthorized, unanticipated, or unintentional modification. Data that is classified under the “availability category” refers to information or services that must be available on a timely basis to meet mission requirements. There is no data handled by the eCB System that falls into the “Confidentiality Category.”

In terms of sensitivity, most of the data handled by the eCB system is considered to be either of Low or Medium Sensitivity.

### **Opportunities for Improvement:**

A sensitivity/criticality assessment should be performed after the determination of any major change to the system, especially if the nature of eCB data changes.

Green

## Risk Assessment and Management

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

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.

### Significance in the SFA Environment:

**Threat:** Management ignorance or underestimation of inherent risks of a system

**Impact:** 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.

### Current Status:

This risk assessment serves to allow a green stoplight for eCB. Whenever a major change to the system occurs, an assessment should be conducted to determine the impact of the new changes on the security posture of the system. This does not necessarily mean an additional independent risk assessment, but rather an analysis to ensure that any additional risks taken on by the modified system are acceptable.

### **Opportunities for Improvement:**

The owners of eCB need to ensure that future risk assessments occur after any major modification to the system or to the organizations policies and procedures, and at least every three years.

**Green**

## Review of Security Controls

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

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.

### Significance in the SFA Environment:

**Threat:** Inappropriate assignment of security resources; vulnerabilities created by lack of controls, improper controls, or controls that are no longer effective as system threats change over time.

**Impact:** 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.

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.

### Current Status:

Again, this survey allows a green stoplight for eCB. However, as new functionality is added and improvements are made to the system, an impact evaluation to the system's security controls should be made. More importantly, as policies and procedures come out, they should be reviewed for their impact on security controls.

### **Opportunities for Improvement:**

Again, the owners of eCB need to ensure that future security control reviews occur after any major modification to the system or to the organization's policies and procedures, and at least every three years. Also, controls should be examined whenever a new connection to another system is added to ensure that no new vulnerabilities exist.

Green

## Rules Of Behavior

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

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.

### Significance in the SFA Environment:

**Threat:** Inappropriate or insecure system usage creates system vulnerabilities, as well as possibly compromising the system itself.

**Impact:** Rules of behavior that define expected and prohibited behavior increase management's confidence that system users are following information security and privacy policies and standards. 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.

### Current Status:

eCB has a fairly in-depth set of rules of behavior governing proper use while accessing the system. The Rules of Behavior list includes language discussing user acknowledgement, privacy expectations, monitoring of computing resources, violations and consequences, manager/supervisor responsibilities, and accepted use principles.

### **Opportunities for Improvement:**

The eCB Rules of Behavior should specifically delineate each user class, from network engineer to desktop user, and indicate their responsibilities when accessing the system. Also, the rules of behavior should include a statement indicating that the rules of behavior will form the basis for security awareness and training. This statement will further demonstrate the importance of knowing and understanding the rules of behavior to the signee.

Lastly, the eCB security plan does indicate annual renewal of the rules of behavior document, but an additional statement should be included to indicate that users must sign the rules of behavior document prior to receiving access to eCB.

Yellow

## Security Life Cycle Planning

[Back to Risk Cycle Illustration](#)

### Standard: NIST Special Pub 800-14, NIST Special Pub 800-18

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.

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

*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.

*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.

*Disposal Phase:* Briefly describe how information is disposed of and how media are sanitized.

### Significance in the SFA Environment:

**Threat:** Inadequate implementation of security controls due to a lack of established security requirements early in the system's life cycle.

**Impact:** 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 system 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:**

For this review, we did not have access to specific lifecycle documentation. We relied on the eCB security plan for information on this topic. The eCB system is presently in the development phase(s) of the life cycle. In each life cycle phase (Development, Testing, and Performance Testing), the eCB system has been physically located within the Virtual Data Center's (VDC) Integrated Technical Architecture (ITA) environment. This environment has stringent security protection, including but not limited to: firewalls, network utilization monitoring, and operator monitoring. In addition, all eCB environments except for the production environment have ID/password protection barriers located at the entry point to the environment, i.e. the IBM HTTP Web Servers. The eCB production system utilizes SSL 2.0 encryption and certification for HTTP transmissions to and from the client system with a sophisticated PIN and institutional numbering system allowing for specific permission and authorization procedures.

## **Opportunities for Improvement:**

eCB should begin using relevant security portions of SFA's SDLC worksheets to ensure that security is properly implemented throughout the remainder of the system's life cycle, and documentation is kept to help validate the fact. In the immediate term, the following issues should be incorporated into the eCB development lifecycle:

- Document the specifications that were used during the development/acquisition phase of the life cycle.
- Document any security requirements that were used during the development/acquisition phase of the life cycle.
- Document appropriate controls with associated evaluation and test procedures before the procurement. When these procedures are available, they should be documented in the eCB security plan.
- Document the security requirements in the solicitation document during the development/acquisition phase of the life cycle.
- Document the requirement to permit updating the security requirements as new threats/vulnerabilities are identified and as new technologies are implemented during this phase. A statement should be included to address new threats and vulnerabilities.

**Yellow**

## Authorize Processing

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

Ensure that a management official authorizes in writing the 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. Management authorization implies accepting the risk of each system used by the application.

### Significance in the SFA Environment:

**Threat:** Lack of acceptance of system risks; management remaining ignorant of residual risks within the system.

**Impact:** 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.

### Current Status:

The eCB security plan indicates that eCB will comply with FIPS 102, Certification and Accreditation. Therefore, a certification and accreditation process should be integrated as soon as possible. eCB is performing the required tasks to obtain an Interim Approval to Operate, such as completing a system security plan and performing a risk assessment. However, no known plan exists for full certification and accreditation.

### Opportunities for Improvement:

eCB should prepare the documentation to receive an interim approval to operate at the next PRR. To receive the full accreditation, the system will have to undergo an appropriate level of security-related testing. Once authorized, ensure that reauthorization occurs at least every three years or upon major change to the system.

**Yellow**

## Personnel Security

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

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

### Significance in the SFA Environment:

**Threat:** Improper access to information by employees; infiltration by known system intruders; increased insider threat.

**Impact:** 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. Given SFA's interactive operating environment, appropriate personnel security is critical to the security posture of the organization. Without adequate personnel security, SFA runs a high risk of security breaches.

## Current Status:

Federal security requirements apply to all contractor and subcontractor personnel participating in the design, operation, maintenance of CBS systems and/or facilities, or who have access to CBS data. The security requirements are defined in *U.S. Department of Education Personnel – Suitability Handbook*, Chapter 2, Number 11. The requirements vary, depending on the sensitivity of the data handled by the employee, and include completion of Federal employment forms and questionnaires, possible investigation by ED, and fingerprinting. Various forms accompany all requests for access.

All personnel accessing eCB data are subject to ED's security investigation. The level of investigation of these personnel is dependent on the sensitivity of the position they hold. Supervisory personnel with sufficient knowledge of duty assignments recommend position sensitivity requirements. By agreement among the eCB Division director, the eCB COTR, and the SFA CSO, the following factors are considered in determining what level of security clearance is granted:

- The individual's access to the system
- The individual's authority to bypass security
- The potential damage the individual could create
- The individual's job responsibilities

eCB has an effective set of management controls that will assist in personnel security. Audit controls have been implemented which specifically search for suspicious activities, ranging from direct attacks on systems to more subtle intrusion attempts. eCB provides training to all employees on their [Rules of Behavior](#), including SFA policies and employee expectations. However, eCB does not adequately provide for separation of duties procedures, termination procedures for a friendly and unfriendly termination, or explain the policy explaining if a user can gain access to the system prior to the background investigation's completion.

## Opportunities for Improvement:

While as a whole eCB's personnel security procedures are solid, eCB should address the above-mentioned issues. Addressing these findings and continually reviewing personnel security procedures will yield high security returns over the life of the system.

**Red**

## Physical and Environmental Protection

[Back to Risk Cycle Illustration](#)

### Standard: NIST Special Pub 800-18

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

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

### Significance in the SFA Environment:

**Threat:** Damage of equipment through natural disasters, accidents, or improper environmental conditions; theft of IT equipment or data; ease of access to sensitive ports or servers.

**Impact:** Physical and environment protections are especially important for a number of reasons: the protection of IT equipment from damage or theft, the isolation of equipment from potential intruders, and the physical monitoring of IT equipment.

### Current Status:

The virtual data center (VDC) in Meriden, CT houses the eCB system. However, no physical security documentation was available for review under this risk assessment. This factor was noted as missing in the security plan as well. Although the VDC has undergone several audits, eCB should understand the location of its equipment and ensure that its equipment is operating in stable environment.

### **Opportunities for Improvement:**

eCB should request a review of VDC's security documentation and include the results of the review in its security plan. A verbal "all is well" from the VDC should not be accepted as an adequate review. The eCB managers are responsible for the system, not the VDC.

**Yellow**

## Production, Input/Output Controls

[Back to Risk Cycle Illustration](#)

### 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:

**Threat:** Mishandling, loss or compromise of sensitive system material, both electronic and paper; corruption of data files by improper input procedures.

**Impact:** SFA systems are complex and 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:

All transactions with the eCampus Based System are logged and stored within the current ITA shared logging functionality both for the application and hardware. The eCampus Based System utilizes the current SAIG enrollment procedures for restricting access and providing authority to the eCB web site. The current Service Level Agreement (SLA) between the Virtual Data Center (VDC) and the Office of Student Financial Aid (SFA) provides for security and handling of off-site data, special storage, and release or destruction dates. However, without reviewing the VDC's documentation on input/output controls, eCB cannot be certain that its specific equipment, media, etc. is appropriately handled, maintained and disposed of.

## **Opportunities for Improvement:**

eCB should increase the granularity of its understanding of its input/output controls. Below are several recommended areas for improvement, each of which should be incorporated into the system security plan.

- Describe the audit trails for receipt of sensitive inputs and outputs. The eCB security plan references SAIG enrollment procedures for restricting access. These procedures should either be described in detail in this plan or should reference the SAIG security plan, including version number, applicable section number, and contact information of the document controller.
- Describe the procedures and controls used for transporting or mailing media or printed output.
- Describe the procedures for sanitizing electronic media for reuse.

**Yellow**

## Contingency Planning

[Back to Risk Cycle Illustration](#)

### 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.

### Significance in the SFA Environment:

**Threat:** Confusion or disorganization exacerbating an emergency situation; unclear or improper procedures compounding problems; extended system outage and loss of system data.

**Impact:** It is vital for SFA to have an established, coherent plan in place that will cover a wide range of possible incidents, from complete catastrophic failures to an application failure. Additionally, this plan needs to be easily available and understandable in the event of an emergency. Obviously, the middle of an actual incident would not be the proper time for either training or testing of the plan.

### Current Status:

ECB relies on the VDC for its contingency plan and disaster recovery. eCB personnel have not reviewed the VDC documentation to ensure eCB was included in the plan.

### **Opportunities for Improvement:**

The eCB security plan should provide additional information for the contingency plan section. For example, eCB relies on other parties (VDC) to respond to contingencies and disasters. Therefore, the eCB security plan should include the version number, date, section and point of contact information for every document eCB will rely on in the event of an emergency. Another alternative is to maintain a copy of the VDC/CSC documentation with the eCB security plan.

Contingency plans should generally be tested yearly. The decision should be based on risk, the amount of change occurring within eCB or the supporting systems, or Departmental requirements. If the plans are tested, simply include a statement in the eCB security plan indicating this fact. eCB should request the testing results from the VDC and the testing schedule in order to ensure eCB will effectively respond to potential contingencies.

Additionally, contingency plans should be created for more likely less-than-catastrophic events. Many of these could be aggregated into different categories of incidents, but there should be resources available to handle all contingencies, accidental or malevolent. Lastly, all plans should be reviewed for the inclusion of SFA points of contact and involvement.

**Green**

## Application Software Maintenance Controls

[Back to Risk Cycle Illustration](#)

### 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:

**Threat:** Improper updates to applications; system degradation resulting from unexpected software incompatibilities; software failure.

**Impact:** 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:

The eCampus Based System uses only Office of Student Financial Aid (SFA) approved software and hardware currently being utilized in a production capacity in the Virtual Data Center (VDC). The Service Level Agreement (SLA) between the VDC and SFA covers software and hardware warranties. The Application was developed under contract and procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production can be found in the eCB Configuration Management Plan. The test uses live data and test plans trace back to the original security requirements. Test results are documented and forwarded to the eCB Project Manager.

## **Opportunities for Improvement:**

SFA's eCB System Security Officer (SSO) 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 SSO to act as the accrediting authority's agent in between certification cycles. The eCB security plan should contain a statement describing the ownership of the software used to operate and support eCB, including if the software was received from another federal agency with the understanding that it is federal government property.

The eCB security plan should reference any SFA policies restricting the use of copyrighted software or shareware.

Periodic audits should be conducted on users computers (PCs) to ensure only legally licensed copies of software are installed. While it is important to maintain audit logs of individual activity, it is also critical to routinely audit these logs. Once this procedure is established, it should be documented in the eCB security plan.

**Green**

## Data Integrity/Validation Controls

[Back to Risk Cycle Illustration](#)

### Standard: NIST Special Pub 800-18

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.

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

### Significance in the SFA Environment:

**Threat:** Hardware failure or user error causing a loss of retrievable data; data entry errors creating application software corruption; system contamination by malignant software; intentional contamination of the system by unauthorized intruders.

**Impact:** 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.

## Current Status:

eCB uses a variety of controls to counter the various threats to data integrity. If an incident affecting system integrity occurs on the CBS system Web server, Support Manager team members will promptly prepare a written report for ED. The report would:

- Identify the owner of the affected resources(s)
- Identify the person(s) involved
- Describe the incident, the surrounding circumstances, and other pertinent information
- Recommend corrective actions
- List the actions taken to prevent a recurrence

If the incident affects the CBS mainframe, the Technical Support Manager and appropriate Mainframe Development team members will prepare the report. Oracle Secure Network Services uses data encryption and check summing so that data cannot be read or altered. See the Department of Education *Network Security Document*, dated April 27, 1999.

Cheyenne Virus Scan NT, Version 4.0.3A, is installed on all personal computers. Each user's system is scanned every time the user logs on the system. If a virus is found on a PC, the user must immediately contact the SSO.

## Opportunities for Improvement:

As noted in the [sensitivity/criticality analysis](#), integrity is the most important security function required for eCB, requiring the most controls and attention. The following opportunities for improved should be addressed:

- Describe in detail tripwire's functionality in the eCB security plan.
- Perform penetration tests as appropriate on the system and ensure there are procedures in place to ensure that it is conducted appropriately. The decision to use penetration tests should be based upon a risk-based decision. Some systems, due to their sensitivity level, do not require penetration tests. Also, the VDC should conduct these tests already.
- If applicable, message authentication procedures should be established to ensure that the sender of a message is known and that the message has not been altered during a transmission.
- Ensure password crackers are used against password files.
- The eCB security plan should describe the details regarding where the tool(s) are placed, the type of processes detected/reported, and the procedures for handling intrusions. Also, a logical and physical diagram of the intrusion detection architecture/design should accompany the description.

**Yellow**

## Documentation

[Back to Risk Cycle Illustration](#)

### Standard: **OMB A-130, NIST Special Pub 800-18**

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.

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.

### Significance in the SFA Environment:

**Threat:** Inconsistent or missing procedures; inability to effectively operate or train because of a lack of established documented procedures.

**Impact:** 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.

### Current Status:

eCB has made a solid initial effort to document the system from the business case to eCB security plan. However, several areas of improvement were identified during this review. Generally, eCB should concentrate on referencing the documentation for the systems eCB relies upon. For example, eCB mentions several plans maintained by the VDC, but does not supply specific information about the documentation (i.e. version number, date, etc).

### **Opportunities for Improvement:**

eCB should review the documentation maintained by the VDC, including the VDC's disaster recovery plan, contingency plan and security plan (in draft). eCB should ensure that its operational needs are met in the VDC documentation. The applicable sections of the VDC documentation should be noted in the eCB security plan.

**Green**

## 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 verifying 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:

**Threat:** Unauthorized access to system, servers, applications, etc.; inadequate procedures for the protection of passwords.

**Impact:** 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:

eCB has a solid identification and authentication foundation protecting against unauthorized entry. In order to access the eCB system, users must be authorized by the Designated Point Administrator (DPA), have a PIN and a TG number and be logging in for a school participating in Campus-Based Programs. The School User or Servicer must be logged onto the Internet and have a web browser open.

The PIN serves as the User's identifier to allow them to access information in systems for the Department of Education. To obtain a PIN, users must go to [www.pin.ed.gov](http://www.pin.ed.gov) to apply. It takes 5-8 business days to for a new PIN to be issued. The PIN contains four characters and is combined with information about the user (such as the first two letters of their last name/Social Security Number to create their unique pin number. To access the eCampus-Based web site, users must have a TG number and it must be associated with the current Award Year. To obtain a TG number, or to get an existing TG number associated with the current Award Year, users must visit the Student Aid Internet Gateway (SAIG) web site. The TG number contains five characters and is associated with a particular school.

## Opportunities for Improvement:

No major areas of opportunity for improvement were identified. The eCB security plan should indicate procedures for ensuring default passwords have been changed. This issue may need to be discussed with VDC personnel. If the VDC personnel claim they have these controls, make sure to obtain the version number, date, and point of contact of the document that contains this information.

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

Organizations should implement logical access control based on policy made by the management officials 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.

### Significance in the SFA Environment:

**Threat:** Unrestricted access to sensitive data or applications; improper usage of another's access privileges.

**Impact:** 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:**

There are controls in place to authorize or restrict the activities of users and personnel within the application/system. There are hardware and software features that are designed to permit only authorized access to or within the application/system, restricting users to authorized transactions and functions, and/or to detect unauthorized activities. However, eCB does not document its logical access controls in enough detail to provide adequate review. There are numerous areas for improvement.

## **Opportunities for Improvement:**

eCB should document its logical access controls in more detail. Below are several areas for improvement:

- Describe the controls in place to authorize or restrict the activities of users and system personnel within the application in greater detail. While the plan indicates the presence of these controls, the eCB security should provide adequate detail.
- Describe authorization controls within the system. While the authentication procedures are described adequately, authorization procedures should be addressed more thoroughly.
- Post a warning banner in accordance with Public Law 99-474. Also, a copy of the new banner should be included in the security plan.
- Explain authorization procedures in greater detail. For example, the eCB security plan should contain authorization language identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more. Potentially, the section on background clearances could be linked to the section discussing authorization procedures.
- Include separation of duties enforcement to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion.
- Describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users. If users are not allowed to delegate their access permissions, this should be documented in the logical access section.
- Reference the VDC documentation that describes the protection employed to prevent unauthorized intrusions due to eCB connection to the Internet.
- Describe the labeling procedures employed to protect sensitive information.

**Green**

## Public Access Controls

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

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.

### Significance in the SFA Environment:

**Threat:** Insecure public access to confidential data.

**Impact:** 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.

### Current Status:

The general public does not access eCB.

### Opportunities for Improvement:

None Applicable

**Green**

## Security Awareness and Training

[Back to Risk Cycle Illustration](#)

**Standard: OMB A-130, NIST Special Pub 800-14**

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 application and the information in it. This training will be in addition to that required for access to a support system.

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

- 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.

## Significance in the SFA Environment:

**Threat:** Ignorance regarding security policies and procedures can create vulnerabilities that are easily exploitable. The best policies will not help unless employees are properly trained, and proper records are kept regarding the training conducted.

**Impact:** 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. Everyone, regardless of their position or function, must understand some privacy and security issues; 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.

## Current Status:

Security training for eCB personnel and eCB support contractors is mission critical to the success of a well-rounded security program. Security training's purpose is to educate all personnel of their responsibility for protecting information assets from unauthorized disclosures, modifications, and destruction. A good security program will have the system's users buy into the concept that they are responsible for the integrity and functioning of mission essential systems by the manner in which they discipline their PC work habits.

Security awareness training starts with the job posting statement that a Security Clearance is required. The statement explains that the Federal security requirements apply to all contractor and subcontractor personnel who participate in the design, operation, or maintenance of CBS systems or facilities or who have access to eCB data. The security requirements are defined in the U. S. Department of Education *Personnel Suitability Handbook*, Chapter 2, Number 11. The requirements vary, depending on the sensitivity of the data handled by the employee, and include completion of Federal employment forms and questionnaires, possible investigation by ED, and fingerprinting.

Upon notification of new eCB employees by the Human Resources Department, the SSO will ensure that all security requirements are fulfilled and that Federal security clearance paperwork is completed and submitted to ED.

### **Opportunities for Improvement:**

Generally, eCB training and awareness preparations are adequate. However, there are a few areas that should be addressed:

- Describe the type and frequency of application-specific training provided to employees and contractor personnel.
- Describe the procedures for assuring that employees and contractor personnel have been provided adequate training.
- Describe the type and frequency of general support system training provided to employees and contractor personnel.

**Green**

## Audit Trails

[Back to Risk Cycle Illustration](#)

### Standard: NIST Special Pub 800-14

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:

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

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.

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

- 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.

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:

**Threat:** Inability to reconstruct or provide evidence regarding an incident; lack of real-time assessment of insecure practices; inability to effectively review audit logs.

**Impact:** 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:

User accountability is tracked through user ID and password. The eCB system monitors users to verify user identities and to ensure personal accountability. The system records each actual user-resource interaction with the user ID and password, which allows each individual's actions to be audited.

Audit trails are designed and implemented to record appropriate information that assists in intrusion detection and remediation. The audit trail includes sufficient information to establish what events occurred, and who or what caused them (type of event, when the event occurred, user ID associated with the event, program or command used to initiate the event). The trace of user actions is limited to FISAP update(s) and provides user name and time of update.

Online audit logs for the eCB system are only accessible by government staff or contractors that have valid id/password combinations for the eCB environment. Staff or contractors can obtain these id/password combinations by following the current procedures for system authorization which requires appropriate sign off by the System Security Office (SSO) for the eCB system. The form used for authorization can be viewed in appendix E.

The confidentiality of audit trail information is protected if it records personal user information.

The appropriate application/system level administrator review audit trails following a known application/system software problem, an unexplained application/system or user problem, or a known violation of existing requirements by a user.

### **Opportunities for Improvement:**

The audit trails for the eCB system should be reviewed on a regular, consistent basis, not only when an incident occurs. Oftentimes, the audit record will be the only indication that an incident has occurred.

ECB should establish a separation of duties policy between security personnel who administer the access control function and those who administer the audit trail be described.

If keystroke monitoring is used in audit trails, organizations should have a written policy and notify users. The Rules of Behavior may be one vehicle for distributing the information. If keystroke monitoring is used, provide reference to the policy and the means of notification. Also indicate whether the Department of Justice has reviewed the policy.

## Conclusions

First and foremost, it is important to note that eCampus Based is a developing system. Therefore, the findings from this risk assessment should be incorporated into the life cycle development of the eCB system. Also, the data the eCB system maintains and transmits is not impacted by the privacy act, nor does it contain national security information. Moreover, eCB does not disburse student aid funds; rather, eCB plays a major role in the allocation of funds. Due to the nature of eCB data, any exploitation will have a very low impact to SFA as a whole, regardless of how likely the threat may occur. For this system, the likelihood of a threat occurring has also been minimized by the existing/planned system security controls, creating an overall risk level of low.

The risks identified within eCB are mostly administrative in nature, and should be fairly easy to incorporate in the near future. This is important, because as eCB moves to full operational capability, it will be vital to have a solid procedural foundation to support any additional risks arising from new system functionality.

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 opportunities for improvement articulated above.

Risk Management Cycle Stage	Issue Area	Recommendation	Priority
Implement Policies and Controls	Authorize Processing	Pursue initial Certification and Accreditation and receive an interim approval to operate (IATO).	1
	Security Life Cycle Planning	Incorporate SFA's Security Life Cycle checklists into the continuous development of eCB.	2
	Contingency Planning	Obtain and review the contingency plan and disaster recovery plan maintained by the VDC. eCB should ensure its business process will be restored at the VDC if a contingency or disaster occurs.	3
	Physical and Environmental Protection	Request and review the physical and environmental documentation from the Virtual Data Center. Include findings in the eCB system security plan.	4
	Personnel Security	Address the multiple findings in the Personnel Security portion of this assessment, including separation of duties procedures, termination procedures for a friendly and unfriendly termination, and explain the policy describing user access prior to a background investigation's completion.	5
	Logical Access Controls	Incorporate the numerous logical access control findings into the eCB security plan.	6
	Production, Input/Output Controls	Increase the granularity of the eCB Input/Output documentation. This area should have detailed controls addressing specific Input/Output security measures.	7
Assess Risks and Determine Needs	Applicable Laws or Regulations	Ensure compliance with all federal and departmental policies and guidelines explicitly noted in the eCB system security plan.	8