REPORT NO. 2010-199
JUNE 2010

DEPARTMENT OF EDUCATION

FEDERAL FAMILY EDUCATION LOAN PROGRAM (FFELP) SYSTEM

Information Technology Operational Audit

For the Period
July 2009 Through March 2010

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

COMMISSIONER OF EDUCATION

Pursuant to Article IX, Section 2 of the State Constitution and Section 20.15, Florida Statutes, the State Board of Education supervises the system of free public education and is the head of the Department of Education. The State Board of Education appoints the Commissioner of Education, who serves as the Executive Director of the Department of Education. Dr. Eric J. Smith served as Commissioner of Education during the audit period.

The audit team leader was Robert McKee, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF EDUCATION

Federal Family Education Loan Program (FFELP) System

SUMMARY

The Federal Family Education Loan Program (FFELP) provides low-cost educational loans to assist students and their parents in paying for the cost of higher education. The FFELP System is a mainframe application used by the Department of Education (Department), Office of Student Financial Assistance (OSFA) to maintain student loan information.

Our audit focused on evaluating the effectiveness of selected Department information technology (IT) general controls and application access controls applicable to the FFELP System for the period July 2009 through March 2010.

The results of our audit are summarized below:

Finding No. 1: The Department's security administration procedures did not address some important aspects of mainframe user account management.

Finding No. 2: Some unnecessary or inappropriate mainframe and FFELP System access privileges existed among OSFA, financial institution, and educational entity staff. Department management did not periodically review the appropriateness of mainframe or FFELP System access privileges.

Finding No. 3: The Department lacked written procedures for the disabling of IT access privileges for former employees and did not disable the access privileges of some former OSFA employees in a timely manner. In addition, contrary to the requirements of the Department of State General Records Schedule for retention of access control records, the Department did not retain FFELP System access control records of former employees.

Finding No. 4: Some temporary OSFA staff shared generic user identifications (IDs) for FFELP System access that may have limited the Department's ability to establish accountability for FFELP System actions.

Finding No. 5: Certain Department security controls related to user authentication needed improvement.

Finding No. 6: The Department had not established a written System Development Life Cycle methodology to govern the development and modification of its application systems. In addition, existing OSFA written procedures did not address certain important aspects of the program change process for the FFELP System.

BACKGROUND

The Department established OSFA pursuant to Section 1001.20(4)d), Florida Statutes. By law, OSFA is responsible for providing access to and administering State and Federal grants, scholarships, and loans to those students seeking financial assistance for postsecondary study pursuant to program criteria and eligibility requirements.

FFELP provides low-cost educational loans authorized by the Higher Education Act to assist students and their parents in paying for the cost of higher education. To obtain an FFELP loan, the student and his or her parents submit a loan application to an educational entity. Upon approval of the application, an FFELP loan is made to the student (borrower) by a participating financial institution. To protect the financial institution from loss in the event of the borrower's death, disability, or default, the loan is guaranteed by a guarantor. Non-profit and State guaranty agencies are established to guarantee student loans made by lenders under FFELP. The Department, through the business users within the program office of OSFA, serves as the State of Florida guaranty agency for FFELP and

provides certain administrative and oversight functions, while the United States Department of Education provides reinsurance to the guaranty agency (Department).

The FFELP System, based on specified criteria, determines whether an educational loan will be guaranteed and, if guaranteed, maintains information relating to the loan. The FFELP System resides on a mainframe computer located at the Northwest Regional Data Center (NWRDC). The Department uses, among other things, mainframe security software to control access to the FFELP System, including application programs and data files.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Security Administration Procedures

Access controls are intended to prevent or detect inappropriate access to computer resources. Effective access controls include security administration procedures that provide tactical guidance on the day-to-day operations of creating, assigning, monitoring, updating, and revoking access privileges.

To access the FFELP System, users were required to first log into the NWRDC mainframe with a valid user account. Mainframe user account management, the process of creating, maintaining, and disabling mainframe user accounts, was performed by OSFA IT staff.

Our audit disclosed that the Department's security administration procedures relating to mainframe user account management did not address some important aspects as described below:

- Specific security administrator steps in creating or disabling user accounts, including which screens are to be used, how login identification codes (IDs) are to be assigned, and specific user account parameters that must be set;
- Descriptions of user ID string types (naming conventions) and how they should be assigned to users (e.g., based on least privileges required for job position and duties); and
- Management of access rules that define access privileges to specific data sets.

As indicated by the access control deficiencies discussed below in Finding Nos. 2 through 5, without written procedures, the risk is increased that controls over mainframe user access may not be followed consistently in a manner pursuant to management's expectations.

Recommendation: The Department should enhance its security administration procedures by documenting management's expectations for managing mainframe user accounts.

Finding No. 2: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to only what is needed in the performance of assigned job responsibilities. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction and promote an appropriate separation of incompatible duties.

As a part of our audit, we reviewed the appropriateness of selected mainframe and FFELP System user accounts. Our audit disclosed that some unnecessary or inappropriate mainframe and FFELP System access privileges existed among OSFA, financial institution, and educational entity staff. These deficiencies, discussed in the following paragraphs, increased the risk that Department data and IT resources could be subject to improper disclosure, modification, or destruction.

Our test of 128 active mainframe user accounts in the OSFA FFELP user and IT groups as of December 7, 2009, identified 33 user accounts that were unnecessary or that had access privileges that were inappropriate for the employees to whom they were assigned. Specifically, of the 33 user accounts:

- 9 had never been used.
- 10 had not been used for 203 to 3,558 days as of December 7, 2009.
- 15 had TSO or JOB privileges that were not necessary for the employees' job duties.
- 7 had inappropriate user ID string assignments.

Our test of 333 active mainframe user accounts in the financial institution and educational entities user groups as of December 7, 2009, identified 311 user accounts that were unnecessary or that had access privileges that were inappropriate for the employees to whom they were assigned. Specifically, of the 311 user accounts:

- 193 had never been used.
- 105 had not been used for 161 to 3,875 days as of December 7, 2009.
- 10 had TSO or JOB privileges that were not necessary for the employees' job duties.
- 16 had inappropriate user ID string assignments.

Our sample of 35 active FFELP System user accounts identified 5 instances of unnecessary or inappropriate access. Specifically:

- 2 FFELP System user accounts assigned to one OSFA employee included unnecessary security administration access privileges, increasing the risk that the privileges will be misused. In response to audit inquiry, Department management indicated that the security administration access has now been removed.
- 2 OSFA employees with programming access privileges also had access privileges that included security administration capabilities, contrary to an appropriate separation of duties.
- 1 OSFA employee with programming access privileges also had update access to the FFELP System in production, contrary to an appropriate separation of duties. In response to audit inquiry, Department management indicated that the update access has now been removed.

We also noted that Department management did not conduct periodic reviews of mainframe or FFELP System user accounts to ensure the appropriateness of access privileges. As demonstrated by the deficiencies described above, the absence of periodic reviews limited Department management's ability to timely detect unnecessary or inappropriate access privileges.

Recommendation: The Department should ensure that mainframe and FFELP System access privileges are appropriately restricted to only what is needed for users to perform their assigned job duties. Additionally, the Department should periodically review active mainframe and FFELP System user accounts to identify and adjust any inappropriate or excessive access privileges.

Finding No. 3: Timely Disabling of Former Employee Access

Effective access controls include provisions for timely disabling employee access privileges when employment terminations occur. Prompt action is necessary to ensure that the access privileges are not misused by the former employee or others.

The Department's practice was for OSFA to notify the Department and OFSA personnel offices, along with OSFA network, FFELP System, and mainframe security administrators when employees are to terminate employment with

OSFA. However, the practice was not documented by the Department in the form of written procedures. As demonstrated in the following paragraphs, the absence of written procedures increases the risk that access will not be timely disabled in a manner pursuant to management's expectations.

The Department did not disable the mainframe access privileges of some former OSFA employees in a timely manner. We reviewed the mainframe user accounts of 23 former OSFA employees who terminated employment between July 1, 2009, and December 7, 2009. Our audit disclosed that the mainframe user accounts for 15 of the 23 former employees included in our test retained mainframe access privileges from 19 to 154 days after the employee termination dates. According to Department management, review of security logs indicated that the access privileges of the former employees had not been used after their terminations. Nevertheless, these conditions increased the risk that the access privileges could be misused by the former employees or others.

In addition, during our test of the mainframe rule sets that define access to OSFA data sets as of December 7, 2009, we identified 14 access rules that provided access to OSFA data sets for suspended or deleted user accounts. Under these conditions, the risk was increased that access privileges may be misused by former employees or others.

Our audit further disclosed that the Department did not retain FFELP System access control records of former employees, contrary to the requirements of the State of Florida, General Records Schedule GS1-SL for State and Local Government Agencies. The General Records Schedule provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment. In the absence of such records, the Department could not demonstrate whether it had timely disabled the FFELP System access privileges of former employees.

Recommendation: The Department should establish written procedures for the timely disabling of former OSFA employee access privileges and retain access control records for the FFELP System in accordance with the requirements of the General Records Schedule.

Finding No. 4: Unique User Identification

The effectiveness of access controls is dependent, in part, on the ability to uniquely identify system users. Unique identification of individual users assists in the assignment of access privileges and provides a mechanism for attributing system actions to the responsible user.

Our audit disclosed that some OSFA temporary staff shared generic login IDs for access to the NWRDC mainframe. Without the unique identification of NWRDC mainframe users, the Department's ability to establish accountability for FFELP System actions may be limited.

Recommendation: The Department should assign unique login IDs to all individual users authorized to access the NWRDC mainframe and the FFELP System.

Finding No. 5: User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that certain Department security controls related to user authentication needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department management of the specific issues. Without adequate security controls related to user authentication, the confidentiality, integrity, and availability of data and IT

resources may be compromised, increasing the risk that Department data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The Department should improve security controls related to user authentication to ensure the confidentiality, integrity, and availability of Department data and IT resources.

Finding No. 6: Program Change Controls

Effective controls over program changes are intended to ensure that all changes are properly authorized, tested, and approved for implementation and that access to and distribution of programs are carefully controlled so that program change control activities are performed as management intended. An appropriate separation of duties with regard to program change controls typically includes provisions for the movement of programs into the production environment being controlled by persons independent of the programmer making the program changes.

The Department had not established a written Departmentwide System Development Life Cycle methodology to govern the development and modification of its application systems. In addition, existing written OSFA procedures did not address the following important aspects of the program change process for the FFELP System:

- The employees who may authorize a change and how authorizations are to be documented;
- How changes will be tested;
- The employees who may approve the implementation of program changes; and
- The employees who may implement the program changes into the production environment.

Our audit disclosed that certain aspects of OSFA's program change control process for the FFELP System needed improvement. Specifically, in a sample of 27 service requests involving 11 program changes and 16 other service requests not involving program changes (e.g., restoring history or correcting loan file, rate, or borrower information), as shown below, 16 of the requests lacked documentation of one or more important program change control activities:

	Documentation of Program Change Requests					
	1	2	3	4	5	6
User Authorization of Change	Y	N	N	N	N	N
User Approval of Testing	N	N	N	N	N	N
Management Approval to Implement	N	Y	N	Y	N	Y

	Documentation of Other Service Requests									
	1	2	3	4	5	6	7	8	9	10
User Authorization of IT Service	Y	Y	N	N	N	Y	N	N	N	Y
User Approval of Testing	N	N	N	N	N	N	Y	Y	N	N

Y	= Documentation Available
N	= Documentation Not Available

Additionally, our audit disclosed that OSFA IT programming staff were granted access by the Department to production programming code and production data that was not required in the performance of their job duties. Under these conditions, the risk is increased of unauthorized changes to production FFELP System programs and data.

As demonstrated by the program change control process deficiencies described above, the absence of comprehensive written program change control procedures increases the risk that appropriate change control practices will not be consistently followed pursuant to management's expectations. Under these conditions, there is an increased risk that unauthorized or improperly functioning changes could be made to the FFELP System, jeopardizing the ongoing integrity of FFELP System data.

Recommendation: The Department should establish a written Departmentwide System Development Life Cycle methodology that provides the minimum expectations for controlling the development and modification of all Department application systems and establish more comprehensive FFELP System program change control procedures to provide increased assurance that only authorized programs and program changes are implemented into the FFELP System.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to the FFELP System in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, and reliability of data; and the safeguarding of IT resources.

The scope of our audit focused on evaluating selected Department IT general controls and application access controls applicable to the FFELP System during the period July 2009 through March 2010 but did not include an evaluation of IT controls at NWRDC.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of FFELP including the program's purpose, goals, and compliance requirements; basic data and business processing flows; IT organizational structure; and management.
- Obtained an understanding of the FFELP System including the computing platforms and related software.
- Obtained an understanding of the logical access controls for the FFELP System including user account administration.
- Observed, tested, and evaluated key processes and procedures related to the security controls for the FFELP System, including user account administration procedures, access authorization, appropriateness of user access, timely removal of access privileges, and periodic review of user access privileges.

- Observed, tested, and evaluated key processes and procedures related to Department network and barrier controls, including user authentication (password) controls.
- Observed, tested, and evaluated key processes and procedures related to the Department program change control processes for making modifications to the FFELP System.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated June 22, 2010, the Commissioner of Education provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

THIS PAGE IS INTENTIONALLY LEFT BLANK

EXHIBIT A
MANAGEMENT'S RESPONSE

FLORIDA DEPARTMENT OF EDUCATION

Dr. Eric J. Smith
Commissioner of Education

Just Read, Florida!

June 22, 2010

David Martin, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

We are pleased to attach the Department's response to the preliminary and tentative audit findings and recommendations for *Information Technology Operational Audit of the Department of Education Federal Family Education Loan Program (FFELP) System* for the period of July 2009 through March 2010.

If you have any questions, please contact Ed Jordan, Inspector General, at 245-9418.

Sincerely,

Dr. Eric J. Smith

ewj/br
Attachment
c: Linda Champion
Martha Asbury
Ron Lauver
Levis Hughes

325 W. GAINES STREET • TALLAHASSEE, FL 32399-0400 • (850) 245-0505 • www.fldoe.org

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Education

Auditing Organization:	**Auditor General, State of Florida**
Audit Title:	**Information Technology Operational Audit of the FFELP System Preliminary and Tentative Findings**
Audit Period:	**July 2009 through March 2010**
Response Due Date:	**June 22, 2010**

Finding No. 1: Security Administration Procedures

Finding:

The Department's security administration procedures did not address some important aspects of mainframe user account management.

Recommendation:

The Department should enhance its security administration procedures by documenting management's expectations for managing mainframe user accounts.

FDOE Response:

Although the auditor's review disclosed areas of risk associated with security administration procedures, the audit results did not uncover any instances of unauthorized access to mainframe data.

FDOE/OSFA procedures for mainframe user account management are being enhanced and strengthened and implementation of these procedures will be thoroughly documented.

Finding No. 2: Appropriateness of Access Privileges

Finding:

Some unnecessary or inappropriate mainframe and FFELP system access privileges existed among OSFA, financial institutions, and educational entity staff. Department management did not periodically review the appropriateness of mainframe FFELP System access privileges.

Recommendation:

The Department should ensure that mainframe and FFELP System access privileges are appropriately restricted to only what is needed for users to perform their assigned job duties. Additionally, the Department should periodically review active mainframe and FFELP System user accounts to identify and adjust any inappropriate or excessive access privileges.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

FDOE Response:

Although the auditor's review disclosed areas of risk associated with mainframe and FFELP System access privileges, the audit did not uncover any instances of unauthorized access to mainframe or FFELP System data.

FDOE/OSFA procedures for user access among DOE/OSFA, financial institutions, and educational entity staff are being enhanced and strengthened, and implementation of these procedures will be thoroughly documented. Additionally, FDOE/OSFA is in the process of creating a security report, which will be reviewed by the FDOE/OSFA Security Manager on a regular basis.

FDOE/OSFA has removed user accounts that were unused or that had not been used over an extended period of time and is in the process of conducting further review to determine if there are additional accounts that should be removed. Security personnel are also reviewing user accounts to determine if there are any with access privileges that are inappropriate for the employees to whom they are assigned. It should be noted that in order to provide the necessary 3-tier backup for all systems, it is sometimes necessary to assign privileges to staff who do not work on these systems as part of their regularly assigned duties to ensure a continuous security administration capability. Any security accounts that are not essential to maintaining adequate security administration capabilities either have been or will be removed.

Finding No. 3: Timely Disabling of Former Employee Access

Finding:

The Department lacked written procedures for the disabling of IT access privileges for former employees and did not disable the access privileges of some former OSFA employees in a timely manner. In addition, contrary to the requirements of the Department of State General Records Schedule for retention of access control records, the Department did not retain FFELP System access control records of former employees.

Recommendation:

The Department should establish written procedures for the timely disabling of former OSFA employee access privileges and retain access control records for the FFELP System in accordance with the requirements of the General Records Schedule.

FDOE Response:

Although the auditor's review disclosed areas of risk associated with former employee access, the audit did not uncover any instances of unauthorized access to mainframe or FFELP System data. This is in part due to an existing procedure which disables access of all former employees to the Department's network at the time of their separation and thus makes it difficult and in most cases impossible, for such former employees to access the FFELP System.

Existing written procedures for terminating access of former employees are being enhanced and strengthened, and implementation of these procedures will be thoroughly documented. Additionally, the access control records will be retained for one year after the employee separates in accordance with the General Records Schedule.

Finding No. 4: Unique User Identification

Finding:

Some temporary OSFA staff shared generic user identifications (IDs) for FFELP System access that may have limited the Department's ability to establish accountability for FFELP System actions.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Recommendation:

The Department should assign unique login IDs to all individual users authorized to access the NWRDC mainframe and the FFELP System.

FDOE Response:

Although the auditor's review disclosed areas of risk associated with temporary employee access, the audit did not uncover any instances of unauthorized access to mainframe or FFELP System data.

Unique login IDs will be assigned to all temporary FDOE/OSFA employees.

Finding No. 5: User Authentication

Finding:

Certain Department security controls related to user authentication needed improvement.

Recommendation:

The Department should improve security controls related to user authentication to ensure the confidentiality, integrity, and availability of Department data and IT resources.

FDOE Response:
Note: Finding 5 is considered CONFIDENTIAL. FDOE/OSFA is taking appropriate steps to address the identified concerns.

Finding No. 6: Program Change Controls

Finding:

The Department had not established a written System Development Life Cycle methodology to govern the development and modification of its application systems. In addition, existing OSFA written procedures did not address certain important aspects of the program change process for the FFELP System.

Recommendation:

The Department should establish a written Department-wide System Development Life Cycle methodology that provides the minimum expectations for controlling the development and modification of all Department application systems and establish more comprehensive FFELP System program change control procedures to provide increased assurance that only authorized programs and program changes are implemented into the FFELP System.

FDOE Response:

Although the auditor's review disclosed areas of risk associated with program change control procedures, the audit did not uncover any instances of implementation of unauthorized programs and program changes.

The Department's Information Systems Development Methodology (ISDM) has been developed and will be implemented by June 30, 2010. The Department-wide ISDM comprehensively addresses all components of a "system development life cycle methodology" including each of the components specifically identified by the auditor. The existing FFELP change control procedures (which include a hard-copy authorization process) are generally consistent with the ISDM and will be enhanced and strengthened as necessary to ensure complete documentation of all program changes.