REPORT NO. 2015-007
AUGUST 2014

DEPARTMENT OF EDUCATION

FEDERAL FAMILY EDUCATION LOAN PROGRAM (FFELP) SYSTEM

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

DEPARTMENT OF EDUCATION

Pursuant to Article IX, Section 2 of the State Constitution and Section 20.15(1), 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. During the period of our audit, the following individuals were appointed:

Pam Stewart, Commissioner of Education	From September 17, 2013
Pam Stewart, Interim Commissioner of Education	August 2, 2013, to September 16, 2013
Tony Bennett, Commissioner of Education	December 12, 2012, to August 1, 2013

The audit team leader was William Tuck, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

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) 412-2722; 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 Department of Education (Department), Office of Student Financial Assistance (OSFA), administers the Federal Family Education Loan Program (FFELP) that provides low-cost educational loans to assist students and their parents in paying for the cost of higher education. OSFA is the designated guaranty agency for the State of Florida for all FFELP loans with first disbursements prior to July 1, 2010, and utilizes the FFELP System, a mainframe-based student loan information system administered by the Northwest Regional Data Center (NWRDC), for this purpose. The FFELP System, in the past, based on specified criteria, determined whether an educational loan would be guaranteed and, if guaranteed, maintained information relating to the loan.

Our operational audit focused on evaluating selected information technology (IT) controls applicable to the FFELP System. We also determined the status of corrective actions regarding selected audit findings included in our report No. 2010-199. Our audit disclosed areas in which enhancements in the FFELP System controls and operational processes were needed. The results of our audit are summarized below:

Finding No. 1: Authorization documentation of access privileges for some users was missing and, in some instances, inaccurate.

Finding No. 2: As similarly noted in our report No. 2010-199, some FFELP System users had unnecessary or inappropriate access privileges.

Finding No. 3: The Department had not performed periodic reviews of user access privileges to the FFELP System.

Finding No. 4: As similarly communicated to Department management in connection with our report No. 2010-199, certain FFELP System security controls related to user authentication needed improvement.

Finding No. 5: As similarly noted in our report No. 2010-199, FFELP System program change management procedures needed improvement.

Finding No. 6: The Department had not completed IT resource categorization as required by Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-2.001(3)(l), Florida Administrative Code.

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 provided and manages low-cost educational loans authorized by the Higher Education Act to assist students and their parents in paying for the cost of higher education. Prior to 2010, through FFELP, private lenders made Federally guaranteed student loans to parents and students. Commercial lenders (e.g., Sallie Mae) used their private capital to finance loans under FFELP but received subsidies from the Federal Government. Upon approval of the application, a FFELP loan was 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 was guaranteed by a guarantor.

[1] Chapter 2014-221, Laws of Florida, effective July 1, 2014, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; pending issues and existing contracts; administrative authority; administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code; trust funds; and unexpended balances of appropriations, allocations, and other funds of the AEIT to the AST.

Nonprofit and state guaranty agencies were established to guarantee student loans made by lenders under FFELP. The Department, through the business users within OSFA's program office, served as the State of Florida's guaranty agency for FFELP and provided certain administrative and oversight functions, while the United States Department of Education provided reinsurance to the guaranty agency. Beginning July 1, 2010, all new student loans are made under the Direct Loan Program whereby the Federal Government lends directly to students. OSFA continues to use the FFELP System to manage and maintain information for all FFELP loans with first disbursements prior to July 1, 2010, and provides customer service to schools, lenders, and borrowers through default prevention, collections, and dissemination of information.

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: Access Authorization Documentation

Effective access authorization controls include, among other things, the use of access authorization forms to document the user access privileges that management has authorized.

We requested access authorization documentation for 40 FFELP System users who had been granted access privileges to the FFELP System during the period July 2013 through February 2014. Our review indicated that the Department did not maintain access authorization forms for some FFELP System users. Specifically, for 29 users, the Department could not provide supporting access authorization forms for the access privileges that had been granted to the users. In addition, access privileges documented on access authorization forms for 6 users did not correspond to the actual access privileges granted to them.

The absence of documentation of management's authorization of user access privileges and incomplete or inaccurate access authorization documentation may limit the Department's ability to ensure that user access privileges do not exceed what is necessary for the accomplishment of user assigned job duties.

Recommendation: The Department should maintain documentation of management's authorization of user access privileges and ensure that the documentation is complete and accurate.

Finding No. 2: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to only what is necessary in the performance of assigned job duties.

Our review of 40 FFELP System users' access privileges during the period July 2013 through February 2014 indicated that 15 users had access privileges that were inappropriate and unnecessary for their assigned job duties. The users were assigned to security groups that provided access to organizational functions outside of the organizational units to which they were assigned. Additionally, 4 of the 40 users had inappropriate "superuser" access privileges that allowed update capability to all of the operational functions in the FFELP System. A similar finding was noted in our report No. 2010-199.

Access to inappropriate and unnecessary functions increases the risk that unauthorized disclosure, modification, or destruction of data and IT resources may occur.

Recommendation: The Department should ensure that FFELP System user access privileges are commensurate with their job duties and enforce an appropriate separation of duties.

Finding No. 3: Periodic Review of Access Privileges

Agency for Enterprise Information Technology (AEIT) Rule 71A-1.007(2), Florida Administrative Code, provides that agency information owners shall review access rights (privileges) periodically based on risk, access account change activity, and error rate. Periodic reviews of user access privileges help ensure that only authorized individuals have access and that the access provided to each user remains appropriate. Department management indicated that periodic reviews of user access privileges to the FFELP System had not been performed, as also indicated by the excessive access privileges noted in Finding No. 2 above. The Department's lack of periodic reviews of access privileges to the FFELP System increases the risk that inappropriate access privileges may not be timely detected or remediated and may result in unauthorized or inappropriate changes to the FFELP System data and related IT resources.

Recommendation: The Department should perform periodic reviews of user access privileges to the FFELP System to ensure the continued appropriateness of assigned access privileges.

Finding No. 4: Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain FFELP System security controls related to user authentication that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising FFELP System data and related IT resources. However, we have notified appropriate Department management of the specific issues. Similar issues were communicated to Department management in connection with our report No. 2010-199. Without adequate security controls related to user authentication, the risk is increased that the confidentiality, integrity, and availability of FFELP System data and related IT resources may be compromised.

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

Finding No. 5: Program Change Management Procedures

Effective program change controls are intended to ensure that all program modifications are properly authorized, tested, and approved for implementation. The effectiveness of ensuring that only approved program changes are implemented is enhanced when program changes that have been moved into the production environment are reviewed for appropriateness. Additionally, the effectiveness of program change controls is enhanced when management's expectations for the control of program changes are documented in the form of written procedures.

As similarly noted in our report No. 2010-199, FFELP System program change controls needed improvement. Specifically, our review of 40 FFELP System program changes during the period July 1, 2013, through January 10, 2014, indicated the following:

- For 1 of 29 program changes requiring user acceptance testing, documentation of user acceptance testing was not available.
- For 1 of 28 program changes requiring approvals, documentation of the approval was not available.
- For 6 of 16 program changes moved into production, the movement of the programs into production was not made by staff independent of the programming staff that coded the program changes.
- The Department did not have logging and monitoring processes in place to ensure that all program changes made to production were properly authorized and approved.

In addition, the *Change Management Process* procedure in support of the Department's Information Systems Development Methodology was still in draft form and had not been finalized and approved by management. This procedure specified critical elements of change management, such as the members of the production control team who were responsible for moving program changes into the production environment. The absence of appropriate program change controls as noted above and program change process procedures approved by management increases the risk that program changes may not be implemented in a manner consistent with management's expectations. Furthermore, without a process for verifying that all program changes that occur in the production environment are properly authorized and approved, the risk is increased that erroneous or unauthorized program changes, should they be moved into the production environment, may not be timely detected by management.

Recommendation: The Department should improve FFELP System program change management procedures to ensure that all program changes moved into production are properly documented, authorized, and approved. The Department should also finalize and approve the *Change Management Process* procedure to ensure that program changes are implemented in a manner consistent with management's expectations.

Finding No. 6: Data Categorization

AEIT Rule 71A-2.001(3)(l), Florida Administrative Code, provides that agencies shall categorize all information and information systems in accordance with Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, to estimate the magnitude of harm that would result from unauthorized access, unauthorized modification or destruction, or loss of availability of a resource. FIPS PUB 199 establishes security categories for both information and information systems.

Our review indicated that the Department's IT risk management activities needed improvement with regard to categorizing IT resources. The Department is currently developing data categorization policies and procedures. However, the Department has not started categorizing its data based on an assessment of the potential impact of a loss of confidentiality, integrity, or availability as prescribed by FIPS PUB 199. Under these conditions, the risk is increased that unmitigated vulnerabilities may result that could impact the operations of the Department and the confidentiality, integrity, and availability of Department data and IT resources.

Recommendation: The Department should continue developing its data categorization policies and procedures.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for those findings disclosed in our report No. 2010-199 that were within the scope of this audit.

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 from December 2013 through March 2014 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 in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources. An additional objective was to determine whether the Department had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2010-199 that were within the scope of this audit.

The scope of our audit focused on evaluating selected IT controls applicable to the FFELP System during the period July 2013 through March 2014. The audit included selected application IT controls, including selected input, processing, and output controls relevant to the FFELP System and selected application-level general IT controls over system modification and logical access to programs and data.

This audit was designed to identify, for the IT system and controls included within the scope of the audit, deficiencies in management's internal controls and IT controls and instances of noncompliance with applicable governing laws, rules, or contracts. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT system and controls included within the scope of our audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the IT system and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the FFELP System's purpose or goals involving compliance requirements.
- Obtained an understanding of the data and business process flows including key sources of data, transactions, and output of the FFELP System.
- Obtained an understanding of the user account management processes for authorizing, creating, modifying, and revoking FFELP System user accounts.
- Obtained an understanding of any significant changes which had occurred including policies, procedures, hardware, software, organizational structure, and personnel related to the FFELP System.
- Evaluated selected FFELP System transaction data input controls as of February 6, 2014. Specifically, we reviewed documentation of the standard coding structure developed by the National Council of Higher Education Resources including the Common Account Maintenance which specifies the type of content, record format, edit checks, and file structure.
- Evaluated selected FFELP System transaction data processing controls as of February 6, 2014. Specifically, we reviewed the adequacy of selected edit routines.
- Evaluated the appropriateness of selected FFELP System transaction data output as of February 6, 2014. Specifically, we reviewed program code used to produce output files, the FFELP file transfer report log, and the file where the nightly reports are stored.
- Evaluated the adequacy of application security management policies and procedures for creating and disabling user accounts.
- Evaluated the effectiveness of program change controls for the FFELP System. Specifically, we evaluated 40 of 240 FFELP service requests between July 1, 2013, and January 10, 2014, for appropriate documentation, authorization, testing, approval for production, and appropriate moves into production. We also evaluated the adequacy of selected program change management procedures.
- Observed and evaluated the appropriateness of FFELP System user identification and authentication mechanisms.
- Evaluated the effectiveness of FFELP System user authorizations in granting appropriate access privileges. Specifically, we evaluated the access privileges of 40 FFELP System users from July 1, 2013, through February 27, 2014, for supporting authorization forms and appropriateness of access to the FFELP System.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe those matters requiring corrective action.

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 August 6, 2014, the Commissioner provided responses to our preliminary and tentative findings. This letter is included at the end of this report as **EXHIBIT A**.

EXHIBIT A
MANAGEMENT'S RESPONSE

August 6, 2014

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

Dear Mr. Martin:

The following responses are offered regarding the preliminary and tentative audit findings issued July 7, 2014, with respect to the information technology operational audit of the Department of Education's Federal Family Education Loan Program (FFELP) System:

Finding No. 1: Authorization documentation of access privileges for some users was missing and, in some instances, inaccurate.

Recommendation: The Department should maintain documentation of management's authorization of user access privileges and ensure that the documentation is complete and accurate.

FDOE Response: Users who had access prior to utilization of the access forms (at the end of 2010) were grandfathered in for each ID utilized. Some users, for example, may have had three IDs, with two being grandfathered in, so no security form was available for those two. During the next quarter, we will conduct an annual review and access will be documented according to employees' access needs.

Finding No. 2: As similarly noted in our report No. 2010-199, some FFELP System users had unnecessary or inappropriate access privileges.

Recommendation: The Department should ensure that FFELP System user access privileges are commensurate with their job duties and enforce an appropriate separation of duties.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

David W. Martin
August 6, 2014
Page Two

FDOE Response: The department ensures that FFELP System user access privileges are commensurate with job duties and enforces an appropriate separation of duties. Clerk IDs are assigned according to the department section in which a user is working unless a change of access is noted on the OSFA System Request Form (if available) due to level of work assignment. Users who had access prior to utilization of the access forms (at the end of 2010) were grandfathered in with access as appropriate to their function, not necessarily their position on the organizational chart. The limited "super user" access is necessary, is tightly controlled and is limited to a few experienced and trusted employees. During the next quarter, we will conduct an annual review and make any necessary changes to access privileges related to changes in work duties.

Finding No. 3: The Department had not performed periodic reviews of user access privileges to the FFELP System.

Recommendation: The Department should perform periodic reviews of user access privileges to the FFELP System to ensure the continued appropriateness of assigned access privileges.

FDOE Response: Access privileges are granted commensurate with job duties and are not excessive in relation to the type of access or the number of users. Access is reviewed based upon changes in staff responsibilities by the supervisor as needed. In addition to these standard reviews, OSFA will also begin to conduct an annual review of all users. Clerk IDs are assigned according to the department section in which a user is working unless a change of access is noted on the OSFA System Request Form due to level of work assignment. Users who had access prior to utilization of the access forms (at the end of 2010) were grandfathered in with access as appropriate to their function, not necessarily their position on the organizational chart.

Finding No. 4: As similarly communicated to Department management in connection with our report No. 2010-199, certain FFELP System security controls related to user authentication needed improvement.

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

FDOE Response: Improvements to user authentication controls are scheduled to occur when the FFELP application transitions from the mainframe. OSFA will continue to closely monitor system access in the interim.

Finding No. 5: As similarly noted in our report No. 2010-199, FFELP System program change management procedures needed improvement.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

David W. Martin
August 6, 2014
Page Three

Recommendation: The Department should improve FFELP System program change management procedures to ensure that all program changes moved into production are properly documented, authorized, and approved. The Department should also finalize and approve the Change Management Process procedure to ensure that program changes are implemented in a manner consistent with management's expectations.

FDOE Response: The department/OSFA has manual logging and monitoring processes in place to ensure that all program changes made to production are properly authorized and approved. The logging process is via the SR system reports. The monitoring of changes is conducted via reconciliation reports reviewed by the business-side. Almost all of the mainframe and web System Request (SR) changes have written documentation (hardcopy or electronic) in addition to being tracked in the SR system with user acceptance indicated by a status of "Testing Accepted" or "Closed." Controls are in place to prohibit programmers from direct access to copy into production, which includes data fixes where the change is copied to the production night cycle via a job. This does not require assistance from staff independent from the program staff. Programmers (who have coded the changes) are not authorized to complete the movement of the programming into production independently with the exception of back-ups who only make moves on an emergency basis, for example if the designated person is unavailable. The department does not maintain separate FFELP System program change management procedures. The department's change management procedures are currently being reviewed and are in a draft status.

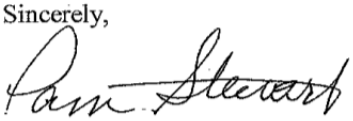
Finding No. 6: The Department had not completed IT resource categorization as required by Agency for Enterprise Information Technology (AEIT) Rule 71A-2.001(3)(l), Florida Administrative Code.

Recommendation: The Department should continue developing its data categorization policies and procedures.

FDOE Response: The department continues to develop its data classification and categorization policy and procedures. This comprehensive policy has been submitted to the Information Security Steering Committee for initial review.

If you need additional information, please contact Martha Asbury at 850-245-0420 or via email at Martha.Asbury@fldoe.org.

Sincerely,



Pam Stewart
Commissioner