STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2018-196
March 2018

DEPARTMENT OF EDUCATION

Federal Family Education Loan Program (FFELP) System

Sherrill F. Norman, CPA
Auditor General

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. Pam Stewart served as Commissioner of Education during our audit period.

The team leader was Faye Smith, CISA, CFE, and the audit was supervised by Tina Greene, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

DEPARTMENT OF EDUCATION

Federal Family Education Loan Program (FFELP) System

SUMMARY

This operational audit of the Department of Education (Department) focused on evaluating selected information technology (IT) controls applicable to the Federal Family Education Loan Program (FFELP) System and included a follow-up on finding Nos. 1 through 5 included in our report No. 2015-007. Although, as discussed in Finding 1, significant constraints were imposed on our audit, we believe the evidence obtained is sufficient and appropriate to provide a reasonable basis for our audit findings. Our audit disclosed the following:

Significant Audit Constraints

Finding 1: Throughout our audit fieldwork, Department management restricted or delayed our access to certain Department records, information, and personnel needed to achieve some of our audit objectives and efficiently conduct the audit.

FFELP System Application Controls

Finding 2: The Department lacked interface procedures that included a complete list of interfaces for the FFELP System.

Finding 3: FFELP System error correction procedures need improvement to ensure that data errors are timely investigated and corrected.

Finding 4: The Department did not demonstrate that the Office of Student Financial Assistance (OSFA) appropriately assigned all defaulted FFELP loans to the United States Department of Education (USDOE) in accordance with the requirements for mandatory assignment (subrogation).

Finding 5: Department records did not demonstrate that appropriate efforts, such as efforts by OSFA staff to reconcile FFELP System and National Student Loan Data System (NSLDS) loan data, were made to ensure the accuracy and completeness of the loan data reported to the USDOE.

FFELP System Access Controls

Finding 6: FFELP System access policies and procedures need improvement to ensure that FFELP System data is adequately protected from unauthorized modification, loss, or disclosure.

Finding 7: Controls for granting access privileges to the FFELP System continue to need improvement to ensure that the access privileges are granted according to appropriately authorized, complete, and accurate access authorization documentation and that such documentation is retained. A similar finding was noted in our report No. 2015-007.

Finding 8: Some controls related to user access privileges granted to the FFELP System and FFELP data need improvement to promote an appropriate separation of duties and restrict users to only those functions necessary for their assigned job duties. A similar finding was noted in our report No. 2015-007.

Finding 9: Department access control procedures need improvement to better ensure that access privileges granted to FFELP System users are timely deactivated when users separate from Department employment or the access is no longer needed.

Finding 10: OSFA's periodic access review procedures for the FFELP System continue to need improvement to ensure that the appropriateness of all users' access privileges is verified. A similar finding was noted in our report No. 2015-007.

Finding 11: Certain Department security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data for the FFELP System and related IT resources continue to need improvement.

FFELP System Change Management Controls

Finding 12: Department change management controls and related procedures for the FFELP System need improvement to ensure that program changes moved into the production environment follow an established change management process and are appropriately authorized, tested, and approved.

NSLDS Access Controls

Finding 13: Department NSLDS access procedures need improvement to demonstrate OSFA's security due diligence in protecting the confidential data in the NSLDS.

Finding 14: Some Department access privileges to the NSLDS were not timely deactivated when the access was no longer needed. In addition, some NSLDS access tokens were not timely collected and deactivated when access was no longer needed.

Finding 15: The periodic reviews of NSLDS user access privileges and monitoring of user access activity performed by the Department need enhancement.

BACKGROUND

The Department of Education (Department) established the Office of Student Financial Assistance (OSFA) pursuant to State law.[1] OSFA is responsible for providing access to and administering State and Federal grants, scholarships, and loans to students seeking financial assistance for postsecondary study pursuant to program criteria and eligibility requirements. The Higher Education Act of 1965 created the Federal Family Education Loan Program (FFELP)[2] to provide incentives for the use of private capital to fund low-interest long-term loans for postsecondary education (such as Stafford, Parental Loans for Undergraduate Students, and Consolidation loans). State and nonprofit organizations, called guaranty agencies, guarantee repayment of the loans in the event of default, death, disability, or other program eligible conditions. OSFA is the guaranty agency for the State of Florida.

Students and their parents applied for student loans from participating financial institutions (lenders) through the FFELP. Upon approval and acceptance of the application and documentation by the lender

[1] Section 1001.20(4)(d), Florida Statutes.

[2] The FFELP is listed in the Catalog of Federal Domestic Assistance as CFDA No. 84.032. For the 2016-17 fiscal year, the FFELP was identified as a major program during the audit of the State of Florida Compliance and Internal Controls Over Financial Reporting and Federal Awards in Accordance with the Uniform Guidance.

and the educational institution, the application was sent to OSFA for guarantee and entry into the FFELP System. The FFELP System resides on a mainframe computer located at the Northwest Regional Data Center.

The Health Care and Education Reconciliation Act of 2010 provided that, after June 30, 2010, no new student loans would be made under the FFELP. Once the Act became law, OSFA guaranteed all loans with first disbursements prior to July 1, 2010, but no longer guaranteed new loans. New educational loans are made under the Direct Loan Program whereby the Federal Government lends directly to the students. OSFA continues to use the FFELP System to manage and maintain information for 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.

OSFA is required to timely submit FFELP System loan data to the National Student Loan Data System (NSLDS). The NSLDS is the United States Department of Education (USDOE) national database of information about loans and grants awarded to students under Title IV of the Higher Education Act of 1965. NSLDS provides a centralized, integrated view of Title IV loans and grants during their complete life cycle, from aid approval through disbursement, repayment, deferment, delinquency, and closure. NSLDS data comes from loan guaranty agencies (such as OSFA), schools, the Direct Loan Program, and other USDOE programs. Each guaranty agency is required by Federal regulations to report to the NSLDS updated loan information submitted to the guaranty agency by lenders and schools.

Federal regulations[3] require OSFA to subrogate (assign) to the USDOE all loans on which the USDOE has paid reinsurance and which meet loan assignment requirements. Additionally, the USDOE Secretary may direct OSFA to assign to the USDOE certain categories of defaulted loans held by OSFA.

According to Department management, there were 4.5 million loans in the FFELP System as of July 1, 2016, of which 2.6 million had been paid in full for 5 years or more. FFELP loan data comprises financial loan data and borrower and student information, including confidential and sensitive personally identifiable information.

FINDINGS AND RECOMMENDATIONS

SIGNIFICANT AUDIT CONSTRAINTS

Finding 1: Auditor Access to Records, Information, and Personnel

State law[4] provides that all officers whose respective offices the Auditor General is authorized to audit or examine shall enter into their records sufficient information for a proper audit or examination, and shall make the same available to the Auditor General on demand. Pursuant to Federal awards audit requirements,[5] auditees are to provide auditors with access to personnel, accounts, books, records, supporting documentation, and other necessary information. Additionally, *Government Auditing*

[3] Title 34, Section 682.409, Code of Federal Regulations.

[4] Section 11.47(1), Florida Statutes.

[5] Title 2, Section 200.508, Code of Federal Regulations, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*.

Standards,[6] issued by the Comptroller General of the United States, provide that, as reflected in applicable laws and regulations, management and officials of government programs are responsible for providing reliable, useful, and timely information for transparency and accountability of these programs and operations. *Government Auditing Standards*[7] require auditors to report any significant constraints imposed on the audit approach by information limitations or scope impairments, including denials or excessive delays of access to certain records or individuals. Also, according to generally accepted auditing standards,[8] examples of significant audit findings include circumstances that cause the auditor significant difficulty in applying necessary audit procedures.

Throughout our audit fieldwork, our requests for access to certain Department records, information, and personnel were not granted or were met with delays, inconsistent or incomplete responses, or documentation that could not be verified as authentic. This lack of cooperation and responsiveness created redundancies in audit requests, postponed or frustrated the performance of audit procedures, and provided our auditors little assurance as to the completeness and accuracy of some Department-provided information. The following are some of the significant constraints imposed on the audit:

- On February 23, 2017, the Chief of OSFA required that we provide him with a written list of all the questions we intended to address during our audit. This stipulation was later revised to a written list of all audit topics. The Chief of OSFA verbally informed our auditors on February 24, 2017, that the auditors would not be allowed to meet with his staff without one of his designated managers being present and that he would instruct Department managers and staff to not respond to any auditor questions (or topics) that had not been provided to him prior to the interview.
- The Assistant Deputy Commissioner of the Division of Finance and Operations required that all our contacts and interactions with OSFA and Division of Technology and Innovation (DTI) management and staff be made in the presence of at least one designated OSFA or DTI manager. In addition, we were required to schedule all meetings and observations and make all data and documentation requests through the designated OSFA or DTI managers. Throughout March 2017 we had numerous discussions with the Assistant Deputy Commissioner of the Division of Finance and Operations during which we conveyed the difficulties we were having scheduling meetings with applicable staff and obtaining necessary documentation for testing. The response continued to be that we must schedule all meetings and observations through the designated managers and that we could not obtain documentation without the Chief of OSFA first reviewing it.
- In some instances, the Assistant Deputy Commissioner of the Division of Finance and Operations and the Chief of OSFA impacted the audit process by intervening or directing other Divisions of the Department how and when to respond to our audit inquiries and requests. For example:
    - We directly requested the Information Security Manager (ISM) to provide certain documentation, but the Assistant Deputy Commissioner of the Division of Finance and Operations responded stating that another person was designated as the liaison for IT. The ISM does not report to the Division of Finance and Operations.
    - During our meeting with a DTI manager, the Chief of OSFA called and instructed him not to provide us any documentation without a written request and to provide the Chief of OSFA with

[6] *Government Auditing Standards*, 2011 Revision, Section 1.02.

[7] *Government Auditing Standards*, 2011 Revision, Section 7.11.

[8] American Institute of Certified Public Accountants, *Codification of Statements on Auditing Standards AU-C* Section 230.A10, *Audit Documentation*.

copies of all requested documentation for review prior to providing the information to us. The DTI manager does not report to the Chief of OSFA.

Examples of audit procedures and objectives that could not be successfully performed or achieved due to the constraints imposed during our audit include:

- On February 22, 2017, we requested read-only access to the Department's network, specifically the network regions containing policies and procedures related to IT security, change management, and the FFELP System and data, to determine whether policies and procedures existed and the availability of the policies and procedures for reference by Department staff. On March 3, 2017, we again requested this access. On March 13, 2017, we received some of the requested policies and were notified that staff were creating a complete list of all OSFA policies and procedures. Although we received the requested direct network access to some DTI policies and procedures, as well as some hard copy and electronic OSFA and DTI policies and procedures, we did not receive the complete list of OSFA policies and procedures and we were never provided direct network read-only access to OSFA policies and procedures and certain other Department policies and procedures needed to achieve our audit objectives.
- On March 14, 2017, we requested documentation to evidence that the DTI security and change control policies and procedures had been appropriately approved by management. The DTI IT Executive Staff Director referred us to the Assistant Deputy Commissioner and the Senior Educational Program Director of the Division of Finance and Operations for this request. Although the Senior Educational Program Director indicated on March 15, 2017, that she was working on our request and we followed up with her on April 17, 2017, the requested documentation was never provided.
- On March 21, 2017, we observed certain NSLDS access procedures performed by the NSLDS primary Destination Point Administrator (DPA)[9] with the OSFA Educational Policy Director and the OSFA Educational Program Director present. For the further analyses required by our audit procedures, we requested that the screen prints, documents, and Excel files created during our observation be provided to us in their original format by the NSLDS primary DPA at the conclusion of our observation through secured File Transfer Protocol (FTP). However, the folder containing the files created during our observation was not provided by the NSLDS primary DPA at the conclusion of our observation as we requested. Instead, the day after our observation, the OSFA Educational Program Director provided a single portable document format (pdf) document combining the screen prints, documents, and files together after the screen prints, documents, and files were reviewed by the Chief of OSFA. As the original format of the files was altered, we were unable to determine the integrity, validity, and completeness of the information included in the document provided.
- On March 21, 2017, we also requested an NSLDS access list and informed the NSLDS primary DPA that we needed to observe the creation of the list when it was generated. Although an NSLDS access list was provided, we were not given the opportunity to observe the creation of the list and, therefore, we had limited assurance as to its completeness and accuracy. We notified the Assistant Deputy Commissioner of the Division of Finance and Operations on March 23, 2017, that our assurance over the reliability of audit evidence is reduced when it is not provided on demand.
- On March 28, 2017, we requested documentation to demonstrate the selection criteria used to select loans for subrogation to the USDOE and the original subrogation list that was generated. On April 19, 2017, we asked to observe the screens and functions in the FFELP System related to subrogation and FFELP outputs, including reports. We followed up on April 21, 2017;

[9] The NSLDS primary DPA is responsible for the users' access to Federal Student Aid systems, to ensure the data provided by these systems is protected according to the Privacy Act of 1974, as amended, as well as to ensure users appropriately access records.

April 25, 2017; April 26, 2017; May 3, 2017; May 11, 2017; and May 25, 2017; however, we were never provided the original subrogation list or allowed to observe, with the responsible individuals, certain FFELP System screens, functions, and output storage locations. Instead, the OSFA Educational Policy Director collected and provided screen prints and documents related to our request and indicated that she would answer any questions and provide any additional screen prints or documents we may need. As a result, we were not given the opportunity to meet with OSFA staff and directly observe the screens, functions, and output storage locations and, therefore, were unable to determine whether the screen prints and documents received were complete and encompassed all the relevant data required to achieve our audit objectives.

- On April 17, 2017, we e-mailed the NSLDS primary DPA requesting specific documentation related to the authorization of NSLDS access privileges granted during the audit period to a specified employee. However, the requested documentation was not provided by the NSLDS primary DPA. Instead, we received a response from the OSFA Educational Policy Director, who was not responsible for NSLDS access. In her response, the OSFA Educational Policy Director stated that she verbally communicated in person with the NSLDS primary DPA to request the access privileges for the specified employee. As neither the requested documentation nor a response from the NSLDS primary DPA was provided, an evaluation of the appropriateness of the access privileges could not be made.
- On April 21, 2017, we requested a meeting with DTI management to observe the creation of, and obtain, various lists of users who had access privileges to FFELP System reports through the datastore repository. We also asked to observe certain network screens and settings to certain data folders related to the security of the FFELP System reports and other output. On May 23, 2017, we requested that DTI management schedule a meeting for us with the staff member who could provide information about the datastore repository and certain data folders, or provide us the staff member's contact information so that we could schedule the meeting. Although we followed up on our request, DTI management did not schedule the requested meeting and, as a result, we were unable to pursue certain inquiries and make the observations necessary to achieve our audit objectives. Access lists with incomplete user information were provided on May 2, 2017; May 26, 2017; and May 30, 2017; by someone other than the manager and staff responsible for securing the access to FFELP System reports and output. We reviewed the documents provided and noted that the lists appeared to be created by copying and pasting information from different locations or documents, thus we were unable to determine the integrity, validity, and completeness of the lists.

Constraints limiting complete and timely access to records, information, and personnel requested for FFELP System audit purposes frustrates the audit process and increases the risk that deficiencies in Department controls applicable to the FFELP System and related IT resources may not be timely identified and corrected. Additionally, the difficulties we encountered in obtaining access to Department records, information, and personnel during audit fieldwork exemplify the need for improved accountability and transparency for the Department's operations and administration of Federal awards and other programs.

Recommendation: We recommend that Department management demonstrate a commitment to accountability, transparency, and compliance with State law by ensuring that access to the records, information, and personnel needed to facilitate a complete and timely audit are provided upon auditor request.

Follow-Up to Management's Response

In her written response, the Commissioner expressed concern that the examples provided in the finding do not reflect the complete set of circumstances surrounding the conduct of the audit and indicated that

the examples illustrate numerous occasions where communication and documentation requests were simply unclear. However, at no time during the audit did Department management advise us of the "numerous occasions" where they found our communication or requests to be unclear. We believe the examples demonstrate the problems encountered due to Department practices restricting our ability to contact the appropriate Department personnel with direct knowledge of the required information.

The Commissioner's response further indicated that Department leadership was not advised in writing either during or at the conclusion of audit fieldwork that any specific requests or documentation requests in general were going to be left unfulfilled. Given our repeated requests, documented in writing as required by the Department, it is not apparent how the Department would not have been aware that our requests were unfulfilled. Further, as the Department insisted that we copy several members of upper management on our requests and that all responses be compiled and reviewed by Department management prior to responding to requests, Department management was well informed of the unfulfilled requests.

The Commissioner's response referenced the "standard practices for all audit engagements" required by the Department and stated that Department leadership was not notified that "any perceived lack of access or failure to provide documentation was interpreted as substantiating this rare and unusual finding." While the Commissioner is correct in that a finding such as this is rarely required, the Audit Supervisor and audit team leader did meet with the Assistant Deputy Commissioner of the Division of Finance and Operations, and the Senior Educational Program Director as early as March 3, 2017, to explain that the restrictive practices required by the Department could result in this finding.

The Commissioner's response also noted that, in late April 2017, the Department contacted us about one of our auditors. At that time the Audit Manager and Audit Supervisor advised the Deputy Commissioner and Assistant Deputy Commissioner of the Division of Finance and Operations that we were not receiving requested information and that Department staff had been uncooperative with our audit team. Although we adjusted the responsibilities of the audit team members in response to the Department's stated concerns, the team continued to experience a lack of cooperation and responsiveness from the Department.

The Commissioner's response implied that we did not discuss the audit findings with Department staff until March 15, 2018, after the written preliminary and tentative findings were delivered to the Department. To the contrary, in addition to numerous telephone conversations, we conducted several in-person meetings with Department management and staff from February 8, 2018, through March 15, 2018, including the exit conference on February 19, 2018, to discuss the findings and to give the Department the opportunity to provide explanations and additional information for our consideration when finalizing the audit findings. As is customary during the audit process, we made appropriate revisions to the preliminary and tentative findings based on the additional information provided.

Finally, the Commissioner's response expressed "a very high level of concern about the documentation, assumptions and conclusions of this finding." We strongly disagree with the characterization that the facts presented in this finding lack appropriate support. In accordance with Government Auditing Standards*, this finding is supported by sufficient, appropriate evidence and the supporting working papers*

were subjected to several levels of review, including review by audit professionals who were not assigned to the audit team.

Notwithstanding the Commissioner's statement that the Department "will continue to do everything possible to ensure that all auditors and our staff are very clear on procedures for each audit," we continue to recommend that Department management ensure that access to the records, information, and personnel needed to facilitate a complete and timely audit are provided upon auditor request. Such access will necessitate that Department management revise the restrictive standard audit practices referenced by the Commissioner in her written response.

FFELP System Application Controls

Finding 2: Interface Procedures

Interface controls include procedures to ensure that interfaces are processed accurately, completely, and timely. Effective interface procedures include a complete list of interfaces, indicate the timing of interface processing, and describe how interfaces are to be processed and reconciled.

As of March 9, 2017, the Department lacked interface processing procedures that included a complete list of FFELP System interfaces. In response to our requests, Department management provided the number of FFELP System interfaces and manually created then gave us two lists of FFELP System interfaces. However, we noted errors in the lists provided and the total number of interfaces Department management provided did not correlate to either list. As such, the Department did not demonstrate, and we were unable to determine, whether the interface lists provided were a complete and accurate listing of all FFELP System interfaces.

The lack of interface processing procedures with a complete list of FFELP System interfaces increases the risk that interfaced data may not be accurately, completely, and timely processed and reconciled as intended by management.

Recommendation: To ensure that interfaced data is accurately, completely, and timely processed and reconciled as intended by Department management, we recommend that Department management establish interface processing procedures that include a complete and accurate list of FFELP System interfaces.

Follow-Up to Management's Response

In her written response, the Commissioner details the various documents provided to satisfy our audit request for a list of all FFELP System interfaces. However, the point of our finding is the importance of having interface procedures that include a complete list of interfaces to reasonably assure that all interfaces are processed accurately, completely, and timely. The Department did not have interface procedures that included a complete list of FFELP System interfaces and, aside from the manually created list of interfaces, the additional documents provided by the Department were computer job schedules and excerpts from a report of nightly jobs processed that did not specifically identify all FFELP System interfaces.

Finding 3: Error Correction Controls

Interface controls address the accurate, complete, and timely processing of information between applications and other source and target systems on an ongoing basis. Interface controls include error handling and reconciliation controls that reasonably assure that all transactions are accounted for and that errors are timely identified, investigated, and corrected.

As discussed in Finding 2, Department records did not support a complete and accurate population of FFELP System interfaces. However, we did identify two significant outgoing interfaces: the NSLDS-Student Aid Internet Gateway (SAIG) Portal and the Subrogation-SAIG Portal interfaces. As part of our audit procedures to evaluate the adequacy of error correction controls, we requested documentation evidencing that errors were timely investigated and corrected for the two interfaces we identified. In response to our request, Department management indicated that documentation was not available to show correspondence between an OSFA employee and the lender regarding lender data error corrections for the NSLDS-SAIG Portal interface because the employee transferred to another position within the Department and the documentation was not retained. Additionally, Department management indicated that errors identified in the Subrogation-SAIG Portal were not corrected until the following year's subrogation processing; however, the Department did not provide documentation to support the correction of errors from the prior year. As further discussed in Finding 4, delays in correcting identified errors could result in the failure to timely assign defaulted loans to the USDOE.

A lack of adequate error correction controls increases the risk that data errors could occur and not be timely investigated and corrected and limits Department management's ability to demonstrate that Department error correction controls are adequate to ensure FFELP System data errors are timely investigated and corrected.

Recommendation: We recommend that Department management improve error correction controls to ensure and document that FFELP System data errors are timely identified, investigated, and corrected.

Follow-Up to Management's Response

The Commissioner's response states that, related to the NSLDS, the discrepancies noted are not interface errors, but are simply differences in the data between OSFA and the USDOE and if the data contains an error, such an error would be a business process error, not an interface error. The response similarly states that, related to subrogation, the list of rejected loans would not be indicative of interface errors. While the Commissioner's response focused on the word "interface," our finding does not refer to interface controls in the strictest definition of interface; rather, the finding refers to the controls related to the complete processing of the interfaced data for the two identified interfaces we selected for testing. Interface and business process controls are linked in that effective controls ensure the timely, accurate, and complete processing of information between feeder and receiving systems and the mainline business processes they support. The point of our finding is that error correction controls need to be implemented or improved to ensure and document that the errors resulting from the process of sending FFELP data to the USDOE systems and receiving error or discrepancy reports in return are timely identified, investigated, and corrected.

Finding 4: Subrogation Processing and Monitoring Controls

Business process application controls include procedures that ensure data is processed completely and accurately, data retains its validity during processing, and effective independent review and monitoring procedures are in place. Federal regulations[10] provide that, unless the USDOE Secretary notifies a guaranty agency in writing that other loans must be assigned to the Secretary, a guaranty agency must assign all defaulted FFELP loans that meet all the following criteria as of April 15 of each year:

- The unpaid principal balance of the loan is at least $100.
- The defaulted loan, as well as other borrower loans, have been held by the agency for at least 5 years.
- A payment has not been received on the loan in the last year.
- A judgment has not been entered on the loan against the borrower.

As part of the Department's subrogation (assignment) process to identify and submit defaulted loans to the USDOE, the DTI runs several computer jobs for various processes. Specifically:

- The forecast and eligibility process is executed annually to forecast subrogation eligibility for the current year and to create the forecast report that identifies all loans potentially eligible to be subrogated. A spreadsheet of all potentially eligible loans is created and sent to OSFA for review. OSFA staff review the spreadsheet and identify for manual removal the loans that do not meet the criteria for assignment. After identifying the loans to be removed from subrogation eligibility, OSFA staff direct the DTI to run the subrogation eligibility report.
- The identification process creates the subrogation eligibility report, the special payment and input files for subrogation, and the manifest report and file to be sent to the USDOE.
- The submit process submits loan files to the USDOE through the SAIG Portal after the loan files have been verified by OSFA staff.
- The accept and reject process is executed after the loan files are received from the USDOE to identify the loans that were accepted and those that were rejected by the USDOE.
- The retrieve file process is executed daily to check the SAIG Portal and retrieve any data found.

As part of our audit procedures, we requested for examination documentation necessary to support the forecast and eligibility process utilized by OSFA for the 2016 loan assignments. However, according to OSFA management, after the subrogation year clears, they do not feel the need to keep certain transition records. As a result, documentation was not retained to corroborate the process used for the 2016 loan assignments or to support the loans manually removed from subrogation eligibility.

In addition, the Department did not provide evidence to demonstrate that subrogation transaction processing errors were timely identified, logged, and resolved, or that the Department implemented adequate audit and monitoring capabilities for subrogation processing and override transactions. In response to our audit inquiries and documentation requests, Department management indicated that:

- OSFA does not maintain the original forecast reports that are generated by the FFELP System and used to identify loans meeting the mandatory assignment criteria.

[10] Title 34, Section 682.409, Code of Federal Regulations.

- OSFA staff directs the DTI to remove from subrogation eligibility the loan records deemed as ineligible for subrogation based on OSFA staff's manual analysis but does not retain evidence of the loan records directed to be removed or the reasons therefor.
- OSFA management approve the subrogation eligibility report after the DTI removes from subrogation eligibility the loan records identified by OSFA as ineligible.
- OSFA staff compile the required hard copy loan documents for those loan records deemed to meet the mandatory assignment criteria, mails the documents to the USDOE, and instructs the DTI to submit the subrogation file electronically to the USDOE.

Because OSFA did not maintain documented evidence of loans manually removed from subrogation eligibility, we were precluded from testing the effectiveness of the Department's business process application controls related to the subrogation process and Department records did not demonstrate that the loans were subrogated in compliance with the Federal requirements for the mandatory assignment of defaulted loans.

Appropriate FFELP System processing and monitoring controls, including the retention of sufficient appropriate documentation to demonstrate compliance with Federal requirements, provide assurance that OSFA appropriately subrogates defaulted loans that meet the USDOE mandatory assignment criteria. In addition, records that support all modifications to subrogation eligibility reports and records and include the date and identify the persons approving and making the changes increase management's ability to hold employees accountable for inappropriate or unauthorized modifications.

Recommendation: We recommend that Department management review and enhance the business process application controls related to the subrogation process to ensure and demonstrate that all defaulted loans meeting the USDOE mandatory assignment criteria are appropriately assigned to the USDOE Secretary as required by Federal regulations. In addition, Department management should ensure that sufficient documentation supporting the subrogation process is retained and available for management review and post audit.

Finding 5: FFELP System Output

Effective output controls include procedures and processes that ensure output generation and distribution are aligned with management's reporting strategy and reasonably ensure output content and availability of output and data are consistent with end-users' needs. Output procedures should also ensure the identification of key outputs that are to be used to track application processing results and assist in the performance of data reconciliations.

Guaranty agencies participating in the FFELP report detailed loan information to the USDOE through the NSLDS, the USDOE central database for student financial assistance. Guaranty agencies with active FFELP loans must provide updated data at least monthly on a schedule established by the USDOE and are responsible for the accurate and timely reporting of data.

As part of our audit procedures, we requested the FFELP System reports or other output reviewed by OSFA staff to track application processing results and assist with reconciling FFELP System data to NSLDS loan data. Although OSFA management provided a list of daily jobs that produce various reports and other forms of output, OSFA management did not identify FFELP System reports or other output reviewed by OSFA staff. Additionally, OSFA management did not provide documentation to evidence that OSFA staff reconciled FFELP System data to NSLDS loan data.

Review and use of appropriate FFELP System reports and other output to track application processing results and reconcile FFELP System data to NSLDS loan data would help ensure the accuracy of the loan data submitted to the USDOE. Absent documentation of efforts to track application processing results and periodic reconciliations of FFELP System data to NSLDS loan data, Department assurances as to the accuracy and completeness of data reported to the USDOE are reduced.

Recommendation: To promote the accuracy and completeness of loan data submitted to the USDOE, we recommend that Department management require the review of appropriate FFELP System reports and other outputs to track application processing results and reconcile FFELP System data to NSLDS loan data. Additionally, we recommend that sufficient documentation be maintained to demonstrate that the tracking efforts and reconciliations were performed.

Follow-Up to Management's Response

The Commissioner's response indicated that the OSFA system included system edits that provided controls to identify and capture all data to be uploaded to the NSLDS and describes, in detail, the process for transmitting the files and subsequent data corrections, including the NSLDS Data Benchmarks tracking the success rate for reconciliation and reporting of data to the NSLDS. However, the point of our finding is that the Department did not provide evidence of the edits or records to demonstrate that appropriate efforts were made to ensure the accuracy and completeness of the loan data reported to the USDOE. While OSFA provided NSLDS reporting statistics, those statistics relate to the data that was transmitted and are not applicable to the control necessary for ensuring the completeness of the data transmitted. Our finding relates to the controls in the FFELP System that ensure that all data that should be transmitted is transmitted.

FFELP System Access Controls

Finding 6: FFELP System Access Policies and Procedures

Effective access controls limit or detect inappropriate access to data and IT resources, thereby protecting the data and IT resources from unauthorized modification, loss, and disclosure. Access control policies and procedures that are developed, documented, disseminated, and periodically updated help to ensure that adequate access controls are in place to protect data and IT resources from unauthorized modification, loss, and disclosure. Policies should address purpose, scope, roles, responsibilities, and compliance issues and procedures should facilitate the implementation of the policies and associated access controls.

Our audit procedures disclosed that FFELP System access policies and procedures needed improvement. Specifically, we noted that:

- Although OSFA developed the *OSFA Security Access Control* and the *OSFA Identification and Authentication (Organizational Users)* policies and procedures, the policies and procedures were in draft form with no effective date or management approval. Additionally, the policies and procedures did not include the time frame within which access should be deactivated after it is no longer needed.
- OSFA developed the *Clerk User ID Description and Screen Access* spreadsheet for the assignment of user accounts (Clerk User ID ranges) to users based on organizational unit. However, the organizational units using the FFELP System were reorganized and the

spreadsheet was not updated to reflect the valid access privileges for the reorganized organizational units. Also, some of the fields on the spreadsheet had not been completed to reflect the valid access privileges (e.g., the spreadsheet did not define override access privileges).

- OSFA grants access to FFELP System users external to the Department for collection and loan maintenance activities. However, OSFA management had not established and implemented procedures for granting access to external FFELP System users and did not maintain a management-approved list of external entity contacts for the external users. The FFELP System security administrator indicated that she grants access based on the access privileges previously given to the external users' entities.

The lack of established access control policies and procedures that are designed to effectively protect FFELP System data, timely disseminated to all appropriate staff, implemented, and updated when appropriate, increases the risk that FFELP System data may be susceptible to unauthorized modification, loss, and disclosure.

Recommendation: We recommend that OSFA management establish access control policies and procedures that ensure FFELP System data is adequately protected from unauthorized modification, loss, and disclosure. Such policies and procedures should be timely disseminated, implemented, and updated, as appropriate.

Follow-Up to Management's Response

While the Commissioner's response states that the two procedures provided to us were approved by the Chief of OSFA and are consistent with Departmentwide policy, the two procedures we were provided did not have an effective date, approval date, or authorizing signature.

Finding 7: Access Authorization Documentation

Agency for State Technology (AST) rules[11] require each agency to manage the identities and credentials for authorized devices and users and establish control measures that address information steward responsibilities which include administering access to systems and data based on documented authorizations. Effective access authorization practices include, among other things, the use and maintenance of access authorization forms to document the user access privileges authorized by management.

The Department uses access authorization forms,[12] signed by the authorizing director, for granting FFELP System user access privileges to Department users. To determine whether FFELP System access privileges granted to Department users were authorized and appropriately assigned, we requested access authorization forms for 12 of the 114 user accounts assigned to 102 Department users who had access privileges to the FFELP System as of April 24, 2017. As illustrated in Table 1, our examination disclosed deficiencies for all 12 selected access authorization forms.

[11] AST Rule 74-2.003(1)(a)6. Florida Administrative Code.

[12] *OSFA System Access Request* forms.

Table 1
Department Staff FFELP System User Access Authorization Forms

Deficiency	1	2	3	4	5	6	7	8	9	10	11	12	Number of Forms with Deficiency
Authorization Form Dated After Access Date						X							**1**
Missing Access Role or Level		X	X	X	X		X	X	X	X	X	X	**10**
Missing Authorizing Director Signature			X		X				X		X	X	**5**
Authorized Role Did Not Match Role Granted	X	X		X	X					X	X		**6**

The Department uses other documentation, such as e-mails, as authorization for granting FFELP System user access privileges to users external to the Department and such access must be approved by the Department's Security Manager. To determine whether the FFELP System access privileges granted to external users were authorized and appropriately assigned, we requested access authorization documentation for 8 of the 33 external users with access privileges to the FFELP System as of April 24, 2017. However, access authorization documentation for 6 of the 8 external users was not provided. The access authorization documentation provided for the other 2 users did not include the approval of the Department's Security Manager and, for 1 of these 2 users, the documentation did not include the specific access role or level authorized.

The maintenance of access authorization documentation that supports the user access privileges granted enhances management's ability to both ensure and demonstrate that access privileges granted to users are authorized and appropriate. A similar finding was noted in our report No. 2015-007.

Recommendation: We recommend that Department management improve controls to ensure that FFELP System access privileges are granted using appropriately authorized and complete access authorization documentation and that such documentation be retained to support the access privileges granted.

Finding 8: Appropriateness of FFELP System Access Privileges

Effective access controls include policies, procedures, and other measures that restrict user access privileges to data and IT resources to only those functions that promote an appropriate separation of duties and are necessary for the user's assigned job duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, and disclosure. As part of our audit, we evaluated FFELP System application access and direct data access privileges.

To evaluate the appropriateness of FFELP System application access privileges granted to Department users, we selected and examined Department records for 12 of the 114 user accounts assigned to 102 Department users and 8 of the 33 user accounts assigned to 33 external users with active access privileges to the FFELP System as of April 24, 2017. Our examination disclosed that, because of inadequately detailed and outdated access role documentation, the appropriateness of the 20 user accounts' access privileges to the FFELP System was not supported. We expanded our audit procedures to include inspection of the assignment of access privileges to access groups and noted instances of inappropriate FFELP System accounts and inappropriate or unnecessary FFELP System access privileges. Specifically:

- The Department established FFELP System access groups that limit FFELP System access privileges and the *Clerk User ID Description and Screen Access* spreadsheet identified the screens assigned to the access groups. Our review of the spreadsheet and user access lists disclosed that the access groups were not defined to ensure an appropriate separation of duties between end-user and IT functions and across all business functions. For example:
  - The Systems access group had 17 user accounts that included both IT and non-IT staff. The Systems access group update access privileges in the FFELP System application were inappropriate for IT staff.
  - Three IT staff had been designated as FFELP System security administrator or backup security administrator and the access privileges assigned to the FFELP System security administrators provided more access than was necessary for security administration duties.
  - Override access privileges for two OSFA staff and one Bureau of the Comptroller (Comptroller) employee provided the users with the override functionality needed to perform assigned duties associated with their business functions. However, the override access privileges also provided the staff with override privileges across business functions.
- 55 FFELP System user accounts with active access privileges to the FFELP System as of April 24, 2017, were not assigned to individuals. These accounts included 45 internal-type user accounts and 10 external-type user accounts and could be used to log on to the FFELP System by anyone who knew the password. In response to our audit inquiries, OSFA management disabled all 55 user accounts.

Similar findings were noted in prior audits, most recently in our report No. 2015-007.

To evaluate the appropriateness of user access privileges that granted direct access to the FFELP System production data, we obtained a list of user accounts that met the access rules for OSFA access to the regions where the FFELP System production data was stored. Our evaluation of the 27 OSFA user accounts as of April 24, 2017, disclosed that all the user accounts had inappropriate access privileges to directly update FFELP System production data outside the FFELP System application controls. Specifically, we found that:

- 21 user accounts were assigned to individuals who did not have a valid business purpose for directly accessing FFELP System production data. These user accounts included 13 accounts assigned to seven programming employees, 3 accounts assigned to a Department security employee, 2 accounts (1 account each) assigned to two OSFA employees, an account assigned to an OSFA contractor, an account assigned to a Comptroller employee, and an account assigned to a Northwest Regional Data Center employee.
- 2 user accounts were assigned to a programming manager and 3 user accounts were assigned to a programming employee who were also performing IT programming and security functions, resulting in the performance of incompatible job duties.
- 1 user account was a generic account that had not been assigned. Department management indicated that this user account was being used by an IT programmer who did not have a valid business purpose for directly accessing FFELP System production data.

Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

Recommendation: We recommend that Department management limit user access privileges to the FFELP System and data to promote an appropriate separation of duties and to restrict users to only those access privileges necessary for the users' assigned job duties.

Finding 9: Timely Deactivation of Access Privileges

AST[13] rules require agency control measures that ensure IT access is removed when an IT resource is no longer required. Prompt action to deactivate access privileges when a user separates from employment or access to the information is no longer required is necessary to help prevent misuse of the access privileges.

OSFA management restricts the use of transaction overrides in the FFELP System by assigning override access privileges. FFELP System override access privileges provide a user with full update capabilities throughout the FFELP System. As part of our audit procedures, we evaluated the three FFELP System user accounts with override access privileges that were in a suspended (i.e., deactivated) status as of April 24, 2017, and were suspended during the period July 1, 2016, through April 24, 2017, for employees who had transferred or separated from Department employment during that period, to determine whether the override access privileges were timely deactivated. Our examination disclosed that one of the three user accounts was for a former employee and was not deactivated until 22 days after the employee's employment separation date.

Timely deactivation of FFELP System override access privileges upon an employee's transfer or separation from Department employment reduces the risk that unauthorized FFELP System access or use by the transferred or former employee, or others, may occur.

Recommendation: We recommend that OSFA management improve procedures to ensure that FFELP System user accounts are timely deactivated upon a user's transfer or separation from Department employment.

Finding 10: Periodic Review of Access Privileges

AST rules[14] require agency control measures that facilitate periodic reviews of access rights with information owners. The frequency of the reviews must be based on system categorization or assessed risk. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user is appropriate. An effective periodic access review consists of identifying the current access privileges of all system users, evaluating the access privileges necessary for the users' current job duties, and ensuring that the authorization forms and actual access privileges reflect the appropriate access privileges.

The OSFA policy for *Security Assessment and Authorization* requires an annual evaluation of all FFELP System security documentation. However, the policy was in draft form without an effective date or management approval and the procedures necessary to execute the policy lacked specific details, such as who should perform the review, when the annual evaluation should be performed, and who should verify access appropriateness.

We examined documentation supporting OSFA management's review of FFELP System access privileges initiated in January 2016. Our audit procedures disclosed that the OSFA review process was

[13] AST Rule 74-2.003(1)(a)8. and (d)3., Florida Administrative Code.

[14] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

not adequate to ensure that only authorized users had access and that the access provided to each user was appropriate. Specifically, we noted that:

- The review was incomplete as it only included selected OSFA users rather than all OSFA users, Department users outside OSFA, and external users.
- The review consisted of providing the most recent *OSFA System Access Request* (authorization) form on file to the user's supervisor and requesting the supervisor to review the request form to verify its accuracy and confirm that the authorized access remained appropriate. The review did not include providing a list of access privileges as defined in the FFELP System (e.g., an access listing generated from the system) to the users' supervisors for review.

Detailed access review procedures approved by management and the periodic performance of a complete review of all FFELP System users' assigned access privileges would increase management's assurance that the access privileges defined for FFELP System users are authorized and appropriate. A similar finding was noted in our report No. 2015-007.

Recommendation: We recommend that OSFA management enhance procedures for the periodic review of all FFELP System user access privileges to ensure that FFELP System user access privileges are authorized and remain appropriate.

Finding 11: Security Controls – User Authentication, Logging and Monitoring, and Protection of Confidential and Exempt Data

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data need 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.

The lack of appropriate FFELP System security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data increases the risk that the confidentiality, integrity, and availability of FFELP System data and related IT resources may be compromised. A similar issue related to user authentication was communicated to Department management in connection with prior audits of the Department, most recently in our report No. 2015-007.

Recommendation: To ensure the confidentiality, integrity, and availability of FFELP System data and related IT resources, we recommend that Department management improve certain FFELP System security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data.

FFELP System Change Management Controls

Finding 12: Change Management Controls

Effective change management controls over program changes ensure that only appropriately authorized, tested, and approved program changes are implemented into the production environment. Further, the effectiveness of change management controls is enhanced when management's expectations for the control of program changes are documented in the form of written procedures and include change

management control processes that are to be followed when program changes are implemented into the production environment.

As part of our audit, we requested the policies and procedures related to program change management for the FFELP System. As similarly noted in previous reports, most recently our report No. 2015-007, we found that FFELP System program change management controls need improvement. Specifically, we noted that:

- Department management had not established accurate and complete program change management policies and procedures. The Office of Applications Development and Support within the DTI established an Information Systems Development Methodology (ISDM) Version 2.0 dated August 2012. The ISDM included standards, processes, and best practices to be used in the development of software applications. We were provided two copies of the ISDM, both identified as Version 2.0. However, the two ISDM documents did not match even though they were identified as the same version. Additional program change management policies, procedures, and process documents provided in response to our audit requests included:
  - Operational Change Management Process, dated March 14, 2005 – Office of Technology and Information Services general and section-specific policies for scheduling, assessing, and following up on changes made to production systems or the environment in which they operate.
  - OSFA Change Management Procedures, dated December 8, 2010 – OSFA procedure with steps to be followed in authorizing service requests (changes to applications), and in authorizing the move of completed programming work to a production environment.
  - OSFA Writing and Submitting a Service Request Training Manual, dated May 2012 – OSFA training manual for entering service requests in the Service Request System.
  - Change Management Process, dated September 1, 2012, revised September 12, 2012 – Office of Applications Development and Support policy to explain the process for implementing code changes in the technology environment.
  - OSFA Configuration Management, not dated – OSFA policy for authorizing, documenting, and controlling changes to the information system.
  - OSFA Application Development Procedures, not dated – OSFA procedure with standards for system developers in creating and maintaining OSFA application systems.

  Our examination of these program change management policies, procedures, and process documents disclosed that management approval was not documented, revision dates were not consistently documented, and some of the documents included inconsistent program change management instructions. For example, we noted that the level of management authorized to sign off on user acceptance testing varied among the documents and included the Business Owner, OSFA Manager, and responsible Director.
- Although Department staff provided logs that documented the movement of program changes into the production environment, according to Department staff, the Department did not use the logs or establish other controls to monitor and reconcile program changes to ensure that all changes were properly authorized, tested, and approved prior to being implemented into the production environment.

Absent effective change management controls that ensure all program changes are authorized, tested, and approved, erroneous or unauthorized program changes may be implemented into the production environment without timely detection.

Recommendation: We recommend that Department management improve change management controls to ensure that a consistent process is used and only authorized, tested, and approved program changes are implemented into the FFELP System production environment.

Follow-Up to Management's Response

The Commissioner's response focused on verification that requested changes are made. However, the point of our finding is that all changes, as recorded in the production log files, should be reconciled to the changes recorded in the change control system to ensure that all changes were authorized, tested, and approved for production. Such a control would help ensure that changes implemented into the production environment have not bypassed the established change control process.

NSLDS ACCESS CONTROLS

Finding 13: NSLDS Access Procedures

The NSLDS contains personal and financial information related to an individual's receipt of Federal student loans authorized under Title IV of the Higher Education Act of 1965, as amended, that is confidential and protected by the Privacy Act of 1974, as amended. The *NSLDS Organization Access Process* provides guaranty agencies with the requirements, acceptable uses, and restrictions for NSLDS online access including established relationship definitions and access certifications. The established relationship definitions specify that access to NSLDS may only be requested for, and granted to, individuals whose purpose for accessing NSLDS includes one of the following:

- Determining an applicant's eligibility for Title IV student loans.
- Billing and collecting on a Title IV loan.
- Enforcing the terms of a Title IV loan.
- Reviewing student enrollment information.
- Ensuring the accuracy of a financial aid or borrower record.
- Assisting with default aversion activities.
- Obtaining default rate information.
- Updating an NSLDS record.
- Updating teacher loan forgiveness and loan discharge information.
- Compliance activities.

The USDOE SAIG was established to allow authorized entities, including FFELP guaranty agencies, to exchange data electronically with the USDOE. SAIG enrollment enables the entity to select services, such as the NSLDS, to receive, submit, view, or update student loan data online and by batch. SAIG participation is required to assign access to the NSLDS. Authentication to the SAIG includes an access token (hardware) assigned to users. As part of the SAIG enrollment, the President, Chief Executive Officer, or designee[15] of the guaranty agency certifies that the agency has provided security due diligence

[15] Florida's designee is the Chief of OSFA.

and verifies that administrative, operational, and technical security controls are in place and are operating as intended.

As part of our audit, we requested documentation, such as established policies and procedures, that demonstrated OSFA had provided security due diligence and had incorporated administrative, operational, and technical security controls to protect the confidential data in the NSLDS. Our examination of OSFA's NSLDS access procedures disclosed that the procedures did not include all relevant steps and were not sufficiently detailed. Specifically, we noted that:

- The initial access registration procedures did not identify:
  - What a supervisor should include in the e-mail when requesting access for a user.
  - How the necessity for NSLDS user access is determined.
  - The training provided to the user.
  - The required access documentation and how long the documentation should be retained.
- The access review procedures did not include:
  - Identification of the USDOE-required security review procedures that are to be routinely performed.
  - When and how supervisors are provided lists of NSLDS access for review of access appropriateness.
  - The supervisors' responsibilities for reviewing NSLDS access.
  - The actions a supervisor is expected to take should inappropriate access be identified.
- The access termination procedures did not include:
  - Detailed instructions for notifying the primary DPA (e.g., via e-mail or other documentation) when an employee with NSLDS access privileges separates from Department employment.
  - Detailed steps to ensure that the SAIG access token is timely collected and disabled at the time the NSLDS access privileges are deactivated.
  - Processes to follow when an OSFA employee with NSLDS access privileges transfers within OSFA or the Department.

Our examination of OSFA's NSLDS access procedures and discussions with OSFA management also disclosed that the procedures were not routinely reviewed, updated, approved by management, or provided to OSFA supervisors. Specifically, we noted that:

- The procedures were written by the previous primary DPA and did not include the creation or last revision date of the documents. In response to our audit inquiry, OSFA management stated that the procedures were not reviewed and approved by management or provided to OSFA supervisors.
- Changes to the access processes were not all reflected in the Department's NSLDS access procedures provided. Specifically, the procedures did not reflect a change in:
  - The NSLDS primary DPA's OSFA position (position of employee designated as the NSLDS primary DPA).
  - The position responsible for requesting and reviewing users' NSLDS access privileges. The procedures specified that the director is responsible; however, the primary DPA and OSFA managers indicated that current processes require the employee's immediate supervisor to request and review NSLDS access.

- How the primary DPA is to be notified of user separations from Department employment.

Access procedures that are reviewed, updated, approved by OSFA management, and provided to OSFA supervisors help demonstrate OSFA's security due diligence in protecting the confidential and protected data in the NSLDS as required by the USDOE.

Recommendation: To demonstrate security due diligence in protecting the confidential data in the NSLDS, we recommend that OSFA management review, update, and approve NSLDS access procedures and provide the procedures to OSFA supervisors.

Finding 14: Timely Deactivation of NSLDS Access Privileges

The *SAIG Enrollment Application* specifies that the primary DPA must ensure that the guaranty agency has a process to inform the primary DPA of any changes in a user's need for access to Federal Student Aid systems, such as the NSLDS, because of changes to job responsibilities or termination of employment. It further specifies that the primary DPA must immediately deactivate or delete user access rights for guaranty agency employees who no longer require access. Additionally, the *NSLDS Organization Access Process* states that the primary DPA is responsible for applying for access and removing access for users who are no longer employed or whose job responsibilities no longer require NSLDS online access. OSFA procedures for employee NSLDS access provide for the former or transferred employee's two-factor authentication (TFA) token to be returned to the primary DPA so that it may be repurposed for another future user.

According to Department records, 35 employees had an active NSLDS user account during the period July 1, 2016, through April 6, 2017, or a TFA token during the period July 1, 2016, through April 21, 2017. We examined the access activities related to the 4 employees who separated from Department employment and the 2 employees who transferred to positions that did not require NSLDS access during the period July 1, 2016, through April 21, 2017, to determine whether the employees' access privileges were timely removed and the related TFA tokens were timely retrieved and deactivated. Our examination disclosed that OSFA's procedures for deactivating NSLDS user accounts and retrieving the TFA tokens need improvement. Specifically, we found that:

- 2 of the 4 employees who separated from Department employment retained NSLDS access privileges for 4 and 5 days respectively after their employment separation dates and also retained their TFA tokens for 3 and 11 days respectively after their separation dates.
- 1 of the 2 transferred employees retained NSLDS access privileges for 163 days and the TFA token for 207 days after his transfer date.

Timely deactivation of NSLDS access privileges and retrieval of the TFA tokens upon an employee's separation from Department employment, transfer, or discontinuation of NSLDS responsibilities reduces the risk of unauthorized access to the confidential data in the NSLDS by former or transferred employees or others.

Recommendation: To help protect the confidential and protected data in the NSLDS, we recommend that OSFA management take appropriate action to ensure that the NSLDS user accounts of former and transferred employees are timely deactivated and the TFA tokens are timely retrieved.

Follow-Up to Management's Response

In her written response, the Commissioner specifies dates that differ from the evidence provided to us during our audit fieldwork. Additionally, she points out that some of the days between employment separation and deactivation of access fell on weekends or holidays. However, unauthorized access can occur at any time, not just during normal business hours. The point of our finding is that, as stated in the SAIG Enrollment Application*, access to Federal Student Aid Systems, such as the NSLDS, must be immediately deactivated for employees no longer requiring access. Deactivating access ensures that the access privileges of former or transferred employees no longer requiring access are not used by the previously assigned user or others to gain access to confidential and sensitive system data.*

Finding 15: Periodic Review of NSLDS Access

The *SAIG Enrollment Application* provides that it is the responsibility of the primary DPA to ensure that all Federal student aid applicant information is protected from access by, or disclosure to, unauthorized personnel. Additional responsibilities of the primary DPA include at least annually validating all user access rights to the NSLDS for the guaranty agency and monitoring the guaranty agency's NSLDS user access by creating reports using the NSLDS Web site.

The *Employee Online NSLDS Access* procedure provides for annual confirmations of employee online NSLDS access by each employee's supervisor. To perform the November 30, 2016, review of active NSLDS user access privileges, the primary DPA manually created an Excel workbook containing spreadsheets, sorted by business section, that listed 28 employees with NSLDS user accounts as of November 30, 2016. According to the primary DPA, the spreadsheets were sent to the applicable supervisors or managers to confirm that the users continued to require access to the NSLDS.

As part of our audit, we evaluated the OSFA processes for the performance of periodic reviews of NSLDS user access privileges and monitoring of user access privileges defined to the NSLDS. We also evaluated documentation supporting the primary DPA's November 30, 2016, annual review of NSLDS user access privileges. Our audit procedures disclosed that the annual NSLDS user access review process needs improvement to ensure compliance with SAIG requirements and the *Employee Online NSLDS Access* procedure. Specifically, we noted that:

- The lists of users were not complete as a user with an active NSLDS user account was not included in the primary DPA's Excel workbook. Therefore, the user's supervisor or manager in the Enterprise Applications Support Section of the DTI was not asked to confirm that the user continued to require access to the NSLDS. In response to our audit inquiry, the OSFA Educational Program Director stated that, at the time of the annual review, the previous primary DPA had a direct daily business relationship with the user and maintained contact with the user's supervisor through system requests and, therefore, personally verified the user's business need and did not include the user on a spreadsheet sent to the supervisors. However, the OSFA Educational Program Director did not provide documentation to demonstrate that the primary DPA verified the user's business need.
- The spreadsheets were not always provided to, and the user account access privileges were not always confirmed by, the applicable supervisors or managers. Specifically:
    - The spreadsheet for 11 user accounts for employees in the Claims and Recovery Section was provided to someone other than the supervisor in the Claims and Recovery Section and OSFA

management did not provide documentation to demonstrate that the privileges were reviewed and approved by the employees' current supervisor or manager. In response to our audit inquiry, the OSFA Educational Policy Director over the Claims and Recovery Section stated that her Administrative Assistant went to each individual supervisor and inquired whether access was needed for each listed individual within their unit. She further stated that, once the need for access was determined, she reviewed the list and requested the Administrative Assistant to forward the response to the primary DPA. However, although we requested, documentation was not provided to support the supervisors' confirmation of the need for the listed users' access or the OSFA Educational Policy Director's review.

- The spreadsheets for 2 user accounts, the manager of the Outreach and Marketing Section and the manager of the Loan Servicing and Forgiveness Section, were provided to the users, rather than the users' supervisors, and the users reviewed and approved their own access privileges.

Additionally, although OSFA management indicated in response to our audit inquiries that the primary DPA was using NSLDS security reports to monitor user access activity on a quarterly basis, OSFA management did not provide examples of the NSLDS security reports or documentation to demonstrate that the primary DPA had monitored user access privileges defined to the NSLDS during the period July 2016 through April 2017.

Without effective periodic access reviews and documented access activity monitoring, management's assurance that user access privileges defined to the NSLDS are authorized and appropriate is limited.

Recommendation: We recommend that OSFA management improve controls and enhance processes to ensure that effective periodic access reviews of NSLDS user access privileges are conducted and that monitoring of NSLDS user access activity is documented.

PRIOR AUDIT FOLLOW-UP

The Department had partially corrected finding Nos. 3 and 5, but had not taken corrective actions for finding Nos. 1, 2, and 4 included in our report No. 2015-007.

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 February 2017 through July 2017 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected IT controls applicable to the Federal Family Education Loan Program (FFELP) System during the period July 2016 through April 2017 and selected actions subsequent thereto. The audit included selected business process application controls over

transaction data interfaces, input, processing, and output; selected application-level general controls over logical access, user identification and authentication, change management, contingency planning, and logical Department access controls to the United States Department of Education (USDOE) National Student Loan Data System (NSLDS). The overall objectives of the 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.
- To determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2015-007 that were applicable to the scope of this audit.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. 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 systems and controls included within the scope of this 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 the audit; obtaining an understanding of the IT systems 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 the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This 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.

Government Auditing Standards[16] state "Auditors should describe the scope of the work performed and any limitations, including issues that would be relevant to likely users, so that they could reasonably interpret the findings, conclusions, and recommendations in the report without being misled. Auditors should also report any significant constraints imposed on the audit approach by information limitations or scope impairments, including denials or excessive delays of access to certain records or individuals." Significant constraints were imposed on the audit including restricted of access to Department records, information, and personnel; delays of access to certain records and information; inconsistent or

[16] *Government Auditing Standards*, 2011 Revision, Section 7.11.

incomplete responses to audit requests; and documentation that could not be verified as authentic. These issues are addressed in Finding 1 of this report.

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 this audit, we:

- Interviewed Department personnel and reviewed FFELP System-related documentation to obtain an understanding of:
  - The application background information including the purpose and goals of the FFELP System.
  - The FFELP System data and business process flows, including key sources of data input and output.
  - The FFELP computing platform including applicable hardware, operating system, database management system, and security software.
  - An overview of the Department's NSLDS access control procedures and processes.
- Evaluated FFELP System business process application controls related to interface, input, processing, and output controls for the FFELP System. Specifically, we:
  - Observed and reviewed screen prints of selected FFELP System input edits for manually entered data made by two Department directors on March 8, 2017, in the test environment, to identify and document selected FFELP System input controls.
  - Observed and inspected FFELP System lockbox deposit input edits and related manual processing controls on March 21, 2017, and April 3, 2017, in relation to lockbox deposits that failed system edits, to identify and document FFELP System deposit edits.
  - Observed and inspected FFELP default claim adjudication processes on April 5, 2017, to identify and document claim input and processing edits.
  - Examined two FFELP loans that had been repaid in full for over 5 years as of July 1, 2016, to evaluate whether the FFELP System input edits would prevent loan payment data from being modified on such loans.
  - Examined borrower's information for one borrower who had a single loan that had been repaid in full for over 5 years as of July 1, 2016, to evaluate whether there were FFELP System input edits to prevent the loan's borrower information from being modified.
  - Inspected a daily lockbox deposit error exception report and related data for March 21, 2017, to evaluate whether FFELP input error handling procedures were in place.
  - Reviewed an excerpt from the February 2017 *Default Aversion Report* and related documentation, to evaluate whether selected default aversion fees were accurately calculated.
  - Reviewed available subrogation documentation to evaluate the business process application controls to evaluate whether FFELP defaulted loans were being subrogated in compliance with Federal regulations.
  - Reviewed available FFELP reports and other output information and documentation, to evaluate the effectiveness of the FFELP System and NSLDS loan data reconciliation processes.

- Evaluated whether the Department maintained a complete and accurate list and reconciliations of interfaces for the FFELP System.
- Reviewed two significant outgoing FFELP System interfaces as of March 22, 2017, to evaluate the adequacy of the interface error correction controls that help ensure the accuracy, completeness, and timeliness of FFELP System interfaced data.

- Evaluated the effectiveness of the Department's transaction logging and monitoring capabilities for FFELP System transactions, including override transactions.
- Evaluated selected FFELP System and IT resources access controls. Specifically, we:
  - Evaluated FFELP System user authorization controls for 12 of the 114 user accounts assigned to 102 Department users and 8 of the 33 user accounts assigned to 33 users external to the Department with FFELP System access privileges as of April 24, 2017.
  - Evaluated FFELP System access policies, procedures, available records, and supporting documentation related to the FFELP System access request and termination procedures and processes. We also examined available access records and supporting documentation to evaluate the appropriateness of 12 Department users' and 8 external users' FFELP System access privileges as of April 24, 2017.
  - Examined FFELP System access documentation to evaluate the appropriateness of access privileges granted to 45 Department and 10 external unassigned user accounts as of April 24, 2017.
  - Reviewed FFELP screen prints and other documents evidencing examples of inappropriate and unnecessary access privileges granted to FFELP System confidential and sensitive loan and borrower personally identifiable information data.
  - Reviewed the FFELP System override and security access roles as of April 24, 2017, to evaluate whether the roles are sufficiently defined at a granular level to help ensure users' access is appropriately separated based on assigned job duties.
  - Reviewed FFELP override access capabilities granted to 2 OSFA and 1 Comptroller users to evaluate the appropriateness of the users' access privileges.
  - Examined the 3 FFELP System user accounts with override access privileges as of April 24, 2017, that had been suspended during the period July 1, 2016, through April 24, 2017, to evaluate whether the override access privileges were timely deactivated for employees who had transferred or separated from the Department.
  - Examined the 27 user IDs, belonging to 13 Department employees, 1 Department contractor, 1 Northwest Regional Data Center employee, and 1 unassigned account that had access granted for directly updating FFELP production data outside of application controls to evaluate the appropriateness of access.
  - Reviewed screen prints as of May 2, 2017; May 26, 2017; and May 30, 2017; evidencing users' access to FFELP System reports and other output to evaluate whether the reports and other output were appropriately restricted to users with a valid business purpose.
  - Evaluated Department FFELP System access review policies, procedures, and processes related to a periodic review of FFELP System access privileges initiated in January 2017.
  - Evaluated user authentication controls related to the FFELP System.
- Evaluated selected FFELP System application change management controls. Specifically, we:
  - Evaluated Department and OSFA change management policies, procedures, and processes in relation to the FFELP System.

- Examined three system change requests relating to six FFELP System changes implemented during the month of October 2016, to evaluate whether the changes were appropriately tested, approved, and implemented.

- Evaluated selected OSFA NSLDS access controls. Specifically, we:
  - Requested a current listing of users with NSLDS access privileges as of March 21, 2017.
  - Reviewed NSLDS access policies and procedures to evaluate whether OSFA had implemented sufficient security controls to demonstrate security due diligence in relation to the protection of NSLDS confidential data.
  - Evaluated OSFA's access review procedures and access review documentation for the annual review of NSLDS access privileges initiated on November 30, 2016.
  - Examined Department records for all 35 employees who had an active NSLDS user account during the period July 1, 2016, through April 6, 2017, or a TFA token during the period July 1, 2016, through April 21, 2017, to evaluate whether access privileges were timely removed and related TFA tokens timely retrieved and deactivated for all employees who separated from Department employment, transferred, or otherwise no longer required the access privileges and TFA tokens.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical 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 the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. 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.

Sherrill F. Norman, CPA
Auditor General

March 28, 2018

Sherrill F. Norman, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

The following revised responses are offered with respect to the information technology operational audit of the Department of Education (department), Federal Family Education Loan Program (FFELP) System.

Significant Audit Constraints

Finding 1: Throughout our audit fieldwork, Department management restricted or delayed our access to certain Department records, information, and personnel needed to achieve some of our audit objectives and efficiently conduct the audit.

Recommendation: We recommend that Department management demonstrate a commitment to accountability, transparency, and compliance with State law by ensuring that access to the records, information, and personnel needed to facilitate a complete and timely audit are provided upon auditor request.

Response: The Florida Department of Education (FLDOE) is fully committed to accountability, transparency and compliance with State law. We believe that this finding reflects a misunderstanding of the FLDOE's long-standing procedures for working relationships with auditors. In addition, we are concerned that the examples provided do not reflect the complete set of circumstances surrounding the conducting of this audit. Lastly, the Department was not notified that documentation for the audit was ultimately lacking, nor informed that any perceived lack of access or failure to provide documentation was being interpreted as substantiating this rare and unusual finding.

For reference, the FLDOE requests the following standard practices for all audit engagements:

1) We ask that requests for documentation, interviews or meetings are made in writing and that specified managers are copied. We do this so that we can keep track of

requests to ensure they are answered timely and completely. For this audit, which involved multiple offices, we included the Deputy Commissioner for Finance and Operations; the Inspector General; an Assistant Deputy Commissioner for Finance and Operations; and the program director for audit resolution. We also request that auditors copy the manager of the applicable program office on such requests.

2) We ask that meetings are coordinated through one of the individuals indicated above and that topics are identified in advance, to ensure that we have appropriate staff to provide the information and that time for staff from both agencies is not wasted.

3) We ask that responsive documents are compiled and reviewed by applicable managers prior to responding to requests. We request this so that documentation is complete and so that a record is maintained for our department for future reference.

4) We ask that FLDOE's provision of responsive documents is documented by electronic record or, in the event that documents are requested in hard-copy, a receipt, particularly where the documents contain personally identifiable information.

These procedures are not intended to frustrate or impede an audit; indeed, these procedures are designed to ensure that responses are timely, accurate, and complete. These procedures are designed to ensure that the individuals with knowledge of the various procedures, policies, and other circumstances contribute to the responses, and to try and minimize confusion between the auditor and agency staff.

The FLDOE acknowledges its obligation to provide the auditors with access to personnel, accounts, books, records, supporting documentation and other information "on demand," and has been able to work with numerous auditors in the past so that our obligations are met and that the audits run smoothly. In the past, our requested practices have been acceptable and the daily working processes between auditors and our staff have maintained a professional environment for each audit to be conducted successfully. This audit, however, was conducted in a very different manner from any of our previous engagements with the Auditor General.

It should be noted that on or about April 27, 2017, after multiple prior attempts to resolve issues surrounding this audit, the FLDOE advised the Auditor General's office that the behavior of the Senior Auditor was untoward and was creating difficulties in completing the audit. In response, the Auditor General's office took steps to ensure that the Senior Auditor had no further contact with FLDOE staff regarding this audit, was not present at FLDOE, and to all appearances was removed from involvement in the audit. After this took place, the other auditors on the Auditor General's staff continued to work with the FLDOE to complete the audit last summer. It was not until this spring when the exit conference was scheduled that the FLDOE learned that prior requests from the Senior Auditor were still active and that outstanding requests were unfulfilled.

The examples provided in this audit finding do not reflect an attempt to frustrate an audit, from which strategy the FLDOE would derive no benefit, but may be support for the decision regarding the Senior Auditor. They do illustrate the numerous occasions where communication and documentation requests were simply unclear. The examples display how the department attempted, in some cases repeatedly, to include documentation that staff believed would, in fact, satisfy what was being requested to the best our understanding.

An opportunity for working conferences to identify gaps in information needed by the remaining auditors after the transition was not provided, nor was the FLDOE leadership advised in writing either during or at the conclusion of the field work of the audit that any specific request or that documentation requests in general were going to be left unfulfilled. More importantly, we were not notified that any perceived lack of access or failure to provide documentation was interpreted as substantiating this finding. Prior to completing field work with a potential scope limitation outstanding, FLDOE leadership would have anticipated notice that the Auditor General's office lacked access or documentation needed to complete the audit. Instead, approximately eight months transpired between the close of field work and the exit conference where FLDOE leadership was so advised.

The preliminary and tentative audit findings were released on February 21, 2018, and the FLDOE's responses were due on March 23, 2018. On March 15, the FLDOE had a meeting with the auditors, during which the preliminary findings were discussed. FLDOE staff were concerned about the discrepancies over the lists of interfaces, and auditors who were present at the meeting indicated they would research this issue to determine whether the finding needed to be revised. In addition, they indicated the finding might need to be revised to indicate that procedures relating to interfaces were lacking, including a list of interfaces. Mid-day on March 23, 2018, the deadline for the FLDOE's response to preliminary findings, the FLDOE verbally received substantive revisions to three findings, providing very little time to make significant revisions to our prepared responses

Given this information, we have a very high level of concern about the documentation, assumptions and conclusions of this finding. At the same time, because the FLDOE is committed to continuous improvement, as well as accountability, transparency and compliance with State law as stated previously, we will continue to do everything possible to ensure that all auditors and our staff are very clear on procedures for each audit. We will examine our communications procedures starting with the entrance conference to ensure that processes are in place and transparent for staff from both agencies to elevate issues of misunderstanding before they result in a finding for our agency.

FFELP System Application Controls

Finding 2: The Department lacked interface procedures including a complete list of interfaces for the FFELP System.

Recommendation: To ensure that interfaced data is accurately, completely, and timely processed and reconciled as intended by Department management, we recommend that Department management ~~ensure that~~ establish interface processing procedures ~~include~~ including a complete and accurate list of FFELP System interfaces.

Response: The current FFELP system operates within an approximately 20 year old mainframe system. The mainframe operates such that a job scheduler is configured to run the code/interfaces that either load or process or output data from the FFELP system. Therefore, the job controller is the mechanism for ensuring that the jobs run accurately, completely and timely as it has prebuilt functionality for whether the job completed successfully, including the number of records processed, and whether the jobs were processed timely. The jobs associated were provided to the auditor on March 14, 2017, during an in-person meeting, and the scheduler was provided on March 28, 2017, by the DTI manager.

An additional control includes Service Request (SR) ticket system that controls how the scheduler is modified. These procedures constitute the controls for the operation of the mainframe. These system controls, in addition to the numerous error-handling procedures acknowledged in other findings, ensure that interfaces are processed accurately, completely and timely. The FLDOE will further document necessary procedures and interfaces.

Upon the auditors' request for a "list of Federal Family Education Loan Program (FFELP) interfaces," the Division of Technology and Innovation (DTI) offered the exhaustive, detailed code for each of the FFELP system jobs that are run, including interfaces, both entering and exiting the system. From this list, DTI constructed a summary list of interfaces in the format sought by the auditor. Upon further discussion with the auditor, the system scheduler was also provided. Any discrepancy between the detailed information initially provided and the manually generated lists was simply due to error in constructing the manual list for the auditors. Discrepancies between the detailed code and the manually generated lists would not adversely impact FLDOE's performance of various tasks because the manually generated lists were produced only for the audit.

Finding 3: FFELP System ~~interface~~ error correction procedures need improvement to ensure that ~~interface~~ data errors are timely investigated and corrected. (Please note this response is to the revised finding communicated verbally on March 23, 2018.)

Recommendation: We recommend that Department management improve ~~interface~~ error correction controls to ensure and document that FFELP System ~~,~~ data errors are timely identified, investigated, and corrected.

Response: OSFA staff stressed to the Senior Auditor that the NSLDS-Student Aid Internet Gateway and Subrogation-SAIG (SAIG) Portal is simply a Secure File Transmission process (SFTP). When OSFA sends data files via SAIG, OSFA receives confirmation that the data was received. No additional interface error controls would be appropriate. All transmission of data are conducted according to USDOE requirements.

Relating to NSLDS, OSFA sends a data file to USDOE. USDOE compares the OSFA data to its data and produces an "error report" that is actually a report of discrepancies in USDOE data compared to OSFA data. Those discrepancies do not relate to any interface errors, but are simply differences in the data. The discrepancies may or may not indicate an error; however, if the data contains an error (in either USDOE data or OSFA data), such an error would be a business process error, not an interface error. NSLDS processing and monitoring controls are addressed in the response to Finding 5.

Similarly, relating to subrogation, OSFA sends a file to USDOE via SAIG. Upon initial receipt, USDOE acknowledges receipt of the electronic files and notifies the FLDOE to forward the paper files. After review of the electronic and paper files (which can take months), USDOE accepts or rejects the subrogation. USDOE then produces an acceptance and rejection report that is transmitted to OSFA. The rejection report lists those loans that were submitted for subrogation, but were rejected as ineligible. Again, the list of rejected loans would not be indicative of interface errors; rather, they are loans USDOE determined were not eligible for subrogation. The reason for the rejection may or may not indicate an error in either USDOE's data or OSFA's data; however, if there is an error in the data on either side, it is a business process error, not an interface error. The reason the "Subrogation Rejected report" is addressed during the next cycle is that the USDOE does not provide the Subrogation Rejected report to the Guarantor until the current year's process has closed. It is therefore, by design of the USDOE's process, impossible to address the rejections until the next cycle. We do note that all loans that are rejected for subrogation remain in the FFELP database as active guarantor-held loans and are, therefore, subject to the FLDOE's processes designed to update and correct data errors. For example, they would be included in the periodic reconciling of FFELP data to NSLDS data.

In response to the auditors' recommendation, OSFA will review the subrogation rejection reports to identify causes of any rejections and, if possible, correct any errors that can be identified. – Subrogation processing and monitoring controls are addressed in the response to Finding 4.

Notably, for both the NSLDS and subrogation processes, it is the USDOE that compares the datasets and produces the "error report" for NSLDS (really, a discrepancy report) and "rejection report" for subrogation. If interface error controls are needed, it would be on the USDOE's side.

In addition to the NSLDS and subrogation processes described above, there is a separate process through which lenders, servicers, or the clearinghouse submit updated student loan data to OSFA to process and submit to NSLDS. There are multiple ways data may be received. The procedures

to verify or reject data will vary according to how the data is received. For example, the receipt of a fax and subsequent system update triggers a review by a supervisor. Upon receipt of data from lenders, services, or the clearinghouse, the FLDOE first updates its database and, subsequently, updates NSLDS through the process described above. In incorporating the updated information from lenders, servicers, or the clearinghouse into the FLDOE database, reports are generated that identify any data that is rejected. Those reports are sent to the lenders, servicers, or the clearinghouse, as applicable, so that rejected data can be addressed.

Finding 4: The Department did not demonstrate that the Office of Student Financial Assistance (OSFA) appropriately assigned all defaulted FFELP loans to the United States Department of Education (USDOE) in accordance with the requirements for mandatory assignment (subrogation).

Recommendation: We recommend that Department management review and enhance the business process application controls related to the subrogation process to ensure and demonstrate that all defaulted loans meeting the USDOE mandatory assignment criteria are appropriately assigned to the USDOE Secretary as required by Federal regulations. In addition, Department management should ensure that sufficient documentation supporting the subrogation process is retained and available for management review and post audit.

Response: In 2017 OSFA and DTI implemented changes to track the iterative steps in determining eligibility for the final Subrogation, in addition to the documentation currently maintained. For 2018, OSFA has started and will continue to refine the tracking process related to this activity.

Finding 5: Department records did not demonstrate that appropriate efforts, such as efforts by OSFA staff to reconcile FFELP System and National Student Loan Data System (NSLDS) loan data, were made to ensure the accuracy and completeness of the loan data reported to the USDOE.

Recommendation: To promote the accuracy and completeness of loan data submitted to the USDOE, we recommend that Department management require the review of appropriate FFELP System reports and other outputs to track application processing results and reconcile FFELP System data to NSLDS loan data. Additionally, we recommend that sufficient documentation be maintained to demonstrate that the tracking efforts and reconciliations were performed.

Response: Each Guaranty Agency is required by federal regulations to report updated information submitted by schools and lenders to NSLDS on at least a monthly basis. OSFA surpasses this federal minimum requirement by reporting to NSLDS semi-monthly.

OSFA's system includes system edits that provide controls to identify and capture all data to be updated to NSLDS. Any rejected data is reviewed by the Destination Point Administrator (PDPA) on a daily basis. The NSLDS Data Benchmarks tracks OSFA's success rate for reconciliation and reporting of data to the NSLDS. OSFA consistently meets and exceeds the required NSLDS Benchmarks. For the reporting period from July 2016 to March 2017, OSFA maintained an average success rate of 99.91% for loans not in repayment status, 98.82% for loans held, and 98.36% for Guaranteed Agency Loans (GA) held. These rates exceed the U.S. Department of Education's established goals of 99.5%, 97.0% and 98.0% respectively. The chart below illustrates OSFA's success rate:

Report Month	**Enrollment Reporting**	**Current Loan Balances**	
	Goals set by the Department(NSLDS): Loans Not In Repayment Status Goal: 99.50	**Lender Held Loans Goal: 97.0**	**GA Held Loans Goal: 98.0**
16-Jul	99.92%	98.7%	98.5%
16-Aug	99.91%	98.7%	98.5%
16-Sep	99.91%	98.7%	98.5%
16-Oct	99.90%	98.7%	98.5%
16-Nov	99.90%	98.7%	98.5%
16-Dec	99.91%	98.9%	98.4%
17-Jan	99.91%	99.0%	98.4%
17-Feb	99.91%	99.0%	97.5%
17-Mar	99.90%	99.0%	98.4%

OSFA also creates and maintains several tracking reports to assist OSFA in reconciliation of discrepancies as provided from NSLDS:

- OSFA's overall number of discrepancies , by type;
-

- Discrepancy report (mislabeled as a "Top Ten Error report" from NSLDS that is really a report of discrepancies noted between FFELP and NSLDS;
- "PMRECS-MMDDYY.txt" report [Presumed Paid In Full (PIF) report, available after each submission);
- "Unreported_loans_MMDDYY.txt" run against FFELP for all loans not reported by the lender manifest or manually updated in over 30 days;
- "THIRD_LVL_ERRS-MMDDYY.txt" that is the Third Level Error report, which includes the type of discrepancy.

These tracking reports are made available on OSFA's shared drive and sent to the supervisor at the beginning of each month. The reports are reviewed and discrepancies are resolved daily, weekly, quarterly, or as information becomes available, depending upon the type of discrepancy and the timeliness of responses from affected parties.

The PDPA performs NSLDS discrepancy review operations daily. This occurs by updates to the FFELP database, updates to NSLDS, Service Requests (SRs) and by correspondence to and from schools, lenders, servicers, or borrowers.

The statement that OSFA did not provide documentation as requested is incorrect. The Department provided the following items, among many others:

- Data Provider Instructions (DPI)
  - ➢ Details electronic process of how files are sent and received; used for creating files transmitted to the NSLDS and provides and overview of how to resolve conflicts and errors
- Error Code List
  - ➢ Listing of code errors and description; used by staff to identify code errors for research
- Field Code list
  - ➢ Listing of data fields where errors occurred; used by staff to identify error fields
- Benchmarks for July 2016 through February 2017
  - ➢ Statistical analysis of agency goals and successes; used by staff for tracking and monitoring progress

- "THIRD_LVL_ERRS-MMDDYY" report from the submission performed on March 10, 2017

  - Electronic File listing detailed account information where errors occurred- produced after each submission; used to create queries and statistical reports for reconciling and resolving discrepancies.

Copies of THIRD_LVL_ERRS-MMDDYY" converted to Excel files made available at auditors request for the following dates: July 11, 2016, October 24, 2016, January 9, 2017, and April 10, 2017.

These documents demonstrate that FFELP System data is compared to NSLDS by sending a file to NSLDS and is conducted semi-monthly, instead of once a month as required by NSLDS. Evidence of tracking efforts and reconciliations being performed are clearly documented in OSFA's extremely low error rate.

As detailed above, FLDOE believes its process already assures the accuracy and completeness of data reported to the USDOE.

The Department also has controls to ensure the information sent to NSLDS is complete. On the day that the NSLDS report (Delta 2 report resulting from extract job EDFJR-188) is sent to NSLDS, a summary report is sent from the FFELP system detailing the number of records sent. The IT programmer waits for the job to complete and then logs into NSLDS web portal to determine how many files were received and to ensure that the number of files received matches the number of files sent. The completeness of the data (correct fields) is addressed in the coding of the job into the FFELP mainframe system.

FFELP System Access Controls

Finding 6: FFELP System access policies and procedures need improvement to ensure that FFELP System data is adequately protected from unauthorized modification, loss, or disclosure.

Recommendation: We recommend that OSFA management establish access control policies and procedures that ensure FFELP System data is adequately protected from unauthorized modification, loss, and disclosure. Such policies and procedures should be timely disseminated, implemented, and updated, as appropriate.

Response: OSFA provided the auditor with the Policy-Security Access Control-NIST AC-1 10-6-16 and the Policy-Identification and Authentication Organizational (Users-NIST IA-10-12-16) that documents existing and approved procedures. While the approval of these procedures and the effective date were not documented, the procedures were approved by OSFA's Bureau Chief and were actually in use. These procedures are consistent with department-wide policy.

The auditor's explanation of the finding does reflect that OSFA has a number of procedures and documentation in place to provide security for our data, including implementation of both department-wide procedures and additional processes specific to OSFA. The FDOE began revising procedures during the audit process and will work to complete the additional controls and procedures that provide additional protections for those data. In addition, the FLDOE will document approval of these procedures and the effective date(s).

Finding 7: Controls for granting access privileges to the FFELP System continue to need improvement to ensure that the access privileges are granted according to appropriately authorized, complete, and accurate access authorization documentation and that such documentation is retained. A similar finding was noted in our report No. 2015-007.

Recommendation: We recommend that Department management improve controls to ensure that FFELP System access privileges are granted using appropriately authorized and complete access authorization documentation and that such documentation be retained to support the access privileges granted.

Response: FLDOE will review and revise its controls to ensure that FFELP System access privileges are granted using appropriately authorized and complete access authorization documentation and that such documentation will be retained to support the access privileges granted.

Finding 8: Some controls related to user access privileges granted to the FFELP System and FFELP data need improvement to promote an appropriate separation of duties and restrict users to only those functions necessary for their assigned job duties. A similar finding was noted in our report No. 2015-007.

Recommendation: We recommend that Department management limit user access privileges to the FFELP System and data to promote an appropriate separation of duties and to restrict users to only those access privileges necessary for the users' assigned job duties.

Response: With respect to override access privileges for two OSFA staff and one Bureau of the Comptroller (Comptroller) employee, OSFA and DTI will work collaboratively to create a log in the system to record instances when overrides have occurred. Additionally, OSFA will work with DTI to develop policies, procedures and practices for improved access controls.

Finding 9: Department access control procedures need improvement to better ensure that access privileges granted to FFELP System users are timely deactivated when users separate from Department employment or the access is no longer needed.

Recommendation: We recommend that OSFA management improve procedures to ensure that FFELP System user accounts are timely deactivated upon a user's transfer or separation from Department employment.

Response: OSFA will make necessary adjustments to ensure timely deactivation.

Finding 10: OSFA's periodic access review procedures for the FFELP System continue to need improvement to ensure that the appropriateness of all users' access privileges is verified. A similar finding was noted in our report No. 2015-007.

Recommendation: We recommend that OSFA management enhance procedures for the periodic review of all FFELP System user access privileges to ensure that FFELP System user access privileges are authorized and remain appropriate.

Response: OSFA maintains its current policies and procedure in The Security Assessment and Authorization policy dated 10-12-16, that documents existing and approved procedures. While approval of these policies and procedures was not documented, these procedures were approved by OSFA's Bureau Chief and were in use during the audit period. As is stated in this report, the Security Assessment and Authorization policy "requires an annual evaluation," which was our normal process as approved by OSFA's Bureau Chief. This document also states the responsible parties for the assessment are Information Technology Management and the OSFA Security Manager. Access appropriateness is discussed in the Security Access Control document—a separate document—and is not a part of Security Assessment and Authorization policy. All security documentation was based on the National Institute of Standards and Technology (NIST) format (provided to the Senior Auditor on March 13, 2017).

OSFA staff does review access procedures including an annual review of all internal (FLDOE) FFELP System users' assigned access privileges. Historically, the reviews were conducted based on the access approval forms; however, the procedures will be improved to utilize the system-generated list of active users to verify that the access granted on the system continues to be appropriate. These procedures will be officially documented. In addition, the FLDOE will ensure that approval and effective dates on the policies and procedures pertaining to periodic access review is documented. The FLDOE will also review these policies and procedures and make any revisions necessary to provide additional details on how the periodic review is to be conducted.

Finding 11: Certain Department security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data for the FFELP System and related IT resources continue to need improvement.

Recommendation: To ensure the confidentiality, integrity, and availability of FFELP System data and related IT resources, we recommend that Department management improve certain FFELP System security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data.

Response: The FLDOE will make necessary improvements to FFELP System security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data.

FFELP System Change Management Controls

Finding 12: Department change management controls and related procedures for the FFELP System need improvement to ensure that program changes moved into the production environment follow an established change management process and are appropriately authorized, tested, and approved.

Recommendation: We recommend that Department management improve change management controls to ensure that a consistent process is used and only authorized, tested, and approved program changes are implemented into the FFELP System production environment.

Response: Management provided OSFA's program change management policies and procedures, which are an accurate and complete reflection of OSFA practices. The OSFA documents were reviewed and authorized by the Bureau Chief. FLDOE and OSFA procedures may differ because OSFA adheres to additional and in some cases higher controls (e.g. the "Move Sheet").

Per the OSFA document Writing a Service Request Training Manual provided to the Senior Auditor, on March 13, 2017, instructions for the user to verify all changes are provided on page 12: "The user should move the Service Request (SR) from Testing or Re-Testing status to Testing Accepted, which authorizes the programmer to have the changes moved into Production." The department will also improve its security controls around logging to ensure that changes in the system are reviewed to verify the requested changes were accurately and completely implemented.

Per the OSFA training manual: "Users are expected to review changes in production, and the Originating Director moves the SR to Closed status."

This does reconcile and verify program changes and ensures proper authorization, testing, approval, and move to production procedures. To further improve the process, OSFA will add a section to the manually generated "production move sheet" indicating the change is complete and ready for production. In addition, OSFA will document the approval and effective date of all change management policies and procedures.

NSLDS Access Controls

Finding 13: Department NSLDS access procedures need improvement to demonstrate OSFA's security due diligence in protecting the confidential data in the NSLDS.

Recommendation: To demonstrate security due diligence in protecting the confidential data in the NSLDS, we recommend that OSFA management review, update, and approve NSLDS access procedures and provide the procedures to OSFA supervisors.

Response: NSLDS is inquiry-only for most users. Other than the PDPA, the secondary PDPA and the Teacher Loan Forgiveness (TLF) representative, limited access is given to the TLF representative for updating TLF awards only.

OSFA follows procedures mandated by NSLDS. The PDPA and supervisors review procedures annually. Updates are made as warranted and as mandated by NSLDS. Procedures provided at the time of the audit included General NSLDS and Guaranty Agency responsibilities, desktop procedures on how to add a user to NSLDS, Employee Online NSLDS Access, Benchmark Information and the NSLDS Guide. These procedures address initial access registration, access review, and access termination procedures.

While staff uses NSLDS procedures provided by USDOE, OSFA also maintains desktop procedures that are approved by unit supervisors (but not executive FLDOE management). These desktop procedures have since been revised in the year since the audit to include additional details from the NSLDS procedures. OSFA will document the approval of these procedures and the distribution of the procedures to all relevant supervisors and staff.

Finding 14: Some Department access privileges to the NSLDS were not timely deactivated when the access was no longer needed. In addition, some NSLDS access tokens were not timely collected and deactivated when access was no longer needed.

Recommendation: To help protect the confidential and protected data in the NSLDS, we recommend that OSFA management take appropriate action to ensure that the NSLDS user accounts of former and transferred employees are timely deactivated and the TFA tokens are timely retrieved.

Response: (Response to Finding 14, as verbally revised on March 27). As noted in the Finding, OSFA maintains procedures that require immediate removal of access for individuals upon change of job duties or termination of employment. These procedures have been followed. OSFA has reviewed the documentation the auditors based this finding on and has several observations:

With respect to 2 of 4 employees who separated from the Department, CR's last day of employment was November 25th but his token was retrieved on his last work day, November 23rd, by the Director, effectively ending his access. The PDPA was out of the office November 23 and all state offices were was closed November 24th - 25th and November 26th- 27th fell on a weekend. The PDPA terminated access immediately upon return on the 28th. LA's last day of employment was March 31st and April 1st-2nd fell on

a weekend. The PDPA terminated access immediately upon return on April 3rd. This employee worked off-site and mailed in her token, received on April 11th.

- User YA – (described in the Finding as having retained access NSLDS access privileges for 163 days and the TFA token for 207 days after his transfer date) This employee was promoted, and he retained his needed access in his new capacity. In this new capacity, YA also served as a back-up and he could be utilized for dual-language needs. His access was ultimately terminated for non-use; however, the access was appropriate while granted. The FLDOE will review the non-use policies to determine if revisions are needed.

As detailed in our above response, FLDOE considers it practices due diligence in safe guarding confidential and protected data.

Finding 15: The periodic reviews of NSLDS user access privileges and monitoring of user access activity performed by the Department need enhancement.

Recommendation: We recommend that OSFA management improve controls and enhance processes to ensure that effective periodic access reviews of NSLDS user access privileges are conducted and that monitoring of NSLDS user access activity is documented.

Response: During the audit period, OSFA maintained and complied with appropriate procedures for periodic reviews of NSLDS access and security reports; however, OSFA acknowledges that the documentation to track these efforts could be improved. In accordance with the recommendation, OSFA will revise its procedures to ensure that OSFA's periodic access reviews of NSLDS user access privileges and OSFA's monitoring of NSLDS user access activity are documented.

If you need additional information, please feel free to contact Martha K. Asbury, Assistant Deputy Commissioner, Finance and Operations, at (850) 245-0420 or via email at Martha.Asbury2@fldoe.org

Sincerely,

Pam Stewart

Pam Stewart
Commissioner

PS/sgf

cc: Linda Champion, Deputy Commissioner, Finance and Operations
Mike Blackburn, Inspector General
Martha Asbury, Assistant Deputy Commissioner, Finance and Operations
Mari Presley, Assistant Deputy Commissioner, Finance and Operations