FLORIDA DEPARTMENT OF EDUCATION
fldoe.org

Pam Stewart
Commissioner of Education

September 30, 2018

Eric Miller
Chief Inspector General
Office of the Chief Inspector General
The Capitol
Tallahassee, Florida 32399-0001

Dear Eric:

In accordance with Section 20.055(5)(h), Florida Statutes, attached is the six month status of corrective actions taken in response to Auditor General Report # 2018-196, Federal Family Education Loan Program (FFELP) System.

If you have any concerns regarding this status report, please contact Mike Blackburn by phone at 245-9418 or by email at mike.blackburn@fldoe.org.

Sincerely,

Pam Stewart

Pam Stewart
Commissioner

Attachment

cc: Mike Blackburn, Inspector General
Martha Asbury, Assistant Deputy Commissioner, Finance, and Operations
Joint Legislative Auditing Committee

Inspector General Mike Blackburn

Department of Education
Office of Inspector General – Internal Audit
Six-Month Status Report on: Federal Family Education Loan Program (FFELP) System
Report # 2018-196 Issued: March 30, 2018
Status as of September 30, 2018

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 as of March 28, 2018: 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.

Response as of September 30, 2018: Consistent with FLDOE's commitment to professionalism, accountability, transparency and compliance with state and federal law and regulations and to ensure auditors receive the necessary access to staff and records, FLDOE has written as set of expectations and protocols designed to ensure requests from auditors are fulfilled in the most expedient and expeditious manner possible. FLDOE will provide these expectations and protocols to key personnel whose programs have been identified for audit prior to any entrance conference.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 establish interface processing procedures that include a complete and accurate list of FFELP System interfaces.

Response as of March 28, 2018: 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.

Response as of September 30, 2018: As of May, 2017, the Division of Technology and Innovation (DTI) reconciled the summary interface input/output list derived from the detail lists which were provided to the auditors. Additionally, the FFELP Technical Operations Manual has been developed and approved.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

Finding 3: FFELP System error correction procedures need improvement to ensure that 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.

Response as of March 28, 2018: 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.

Response as of September 30, 2018: OSFA and the Division of Technology and Innovation (DTI) instituted changes to the Error Report database to include information on the date the error was worked, detail concerning the error, and the date the correction was completed. A procedure to generate a monthly report was instituted to ensure the accuracy and success of the corrections.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 as of March 28, 2018: 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.

Response as of September 30, 2018: In 2017 OSFA and DTI implemented changes to track the iterative steps in determining eligibility for final Subrogation. Documentation of these steps began at the beginning of the subrogation process in April 2018 and the files demonstrating this process are being placed in one specific folder on a secure drive named "Subrogation 20CY."

Tracking this process requires the Claims & Recovery Director to submit Service Requests (SR) to IT for those accounts that management deems appropriate to remove from eligibility based on ineligibility criteria. The Claims & Recovery Director will attach documentation to validate these removals to the SR.

Written procedures for this process have been prepared.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 as of March 28, 2018: 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.

Response as of September 30, 2018: To promote the accuracy and completeness of loan data submitted to the USDOE, IT staff began to provide the Destination Point Administrator (PDPA) with successful submission record counts. Once the submission is received and processed by National Student Loan Data System (NSLDS) and error reports are then returned to OSFA, IT staff will advise of completion of the submission and availability of error reports. These files are now reviewed and maintained in a folder which affords limited access to ensure confidentiality.

Effective July 2017, a monthly reconciliation report was created to monitor and compare NSLDS vs FFELP data for completeness and accuracy.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 as of March 28, 2018: 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).

Response as of September 30, 2018: Beginning in October 2017, DTI changed the management structure of staff and functions that handle system access for the FFELP system to report to the Access Management group under DTI and implemented training and mentoring of new DTI Access Management staff in January 2018. Additionally updated FFELP System Access procedures have been developed and approved.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 as of March 28, 2018: 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.

Response as of September 30, 2018: OSFA reviewed and revised 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 as of June 30, 2018.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 as of March 28, 2018: 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.

Response as of September 30, 2018: OSFA worked with DTI to develop policies, procedures, and practices for improved access controls that define IT and Non-IT staff roles and modify the application process with an annual review, including the production of reports and implementing standard DTI requests for Application ID procedures through DOE's Helpdesk. DTI has taken the additional steps towards the separation of duties: performed an audit of the Clerk ID accounts in the FFELP Mainframe application; verified the accuracy of the reports and the correctness of the user accounts form on file for the FFELP Mainframe application; revised the security forms for the multiple OSFA environments and are located in the approved FFELP Technical Operation Manual Appendix Pgs 75-76 (FFELP NWRDC Mainframe FFELP Web Applications (OSFA Intranet); and updated the security roles in the .Net FFELP Applications.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 as of March 28, 2018: OSFA will make necessary adjustments to ensure timely deactivation.

Response as of September 30, 2018: OSFA has made updates to access control procedures to ensure that the FFELP System user accounts are timely deactivated upon a user's transfer or separation from the Department. Furthermore, adjustments have been made to ensure timely deactivation of access privileges when those privileges are no longer needed by existing staff.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 as of March 28, 2018: 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.

Response as of September 30, 2018: OSFA has improved procedures to utilize a system-generated list of active users and their access as compared to staff job requirements to verify that the access granted to the system continues to be appropriate. These procedures include details on how the periodic review is to be conducted and approvals obtained. This review will be conducted on an annual basis.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 as of March 28, 2018: 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.

Response as of September 30, 2018: In March 2018, OSFA and DTI began to make updates to FFELP System security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data. These updates include, the FFELP Application forces users to change passwords every 30-90 days, changed FFLEP Application password requirements from a minimum of 3 characters to 8; rewrote the Application Clerk ID to (a) put controls in place to enforce password complexity, (b) prevent passwords from being changed multiple times during the same day, (c) maintain a history of reused passwords, and (d) created a logging procedure to circumvent invalid logging out and logging back in to reset the invalid logon attempts counter; eliminated the ability to query the application control table for the clerk ID and the review of training materials to ensure no PII is included.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 as of March 28, 2018: 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.

Response as of September 30, 2018: OSFA is documenting the approval and effective date of OSFA's change management policies and procedures through the department's Service Request System (SRS). OSFA has updated the Procedures for SRS to ensure that change requests are tracked from their origin, authorized, tested and approved.

In certain circumstances it may be necessary to bypass the normal service request process and make emergency changes to a system, program or application that operate outside of the normal business hours (8am to 5pm).

An emergency change is one required to correct an existing outage, fatal error, disruption in existing service, system that has crashed or stopped functioning, or to correct performance on a system that is seriously impeding service to the client. The problem or failure has already occurred and we have no option except to take measures that will correct it.

A retroactive service request ticket must be completed and approved by the close of the next business day when an emergency change is implemented.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 as of March 28, 2018: 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.

Response as of September 30, 2018: As noted above, OSFA has updated its procedures to ensure due diligence in protecting the confidential data in the NSLDS.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 as of March 28, 2018: (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.

Response as of September 30, 2018: OSFA has updated procedures to include the process of terminating a user's NSLDS access. OSFA ensures that the NSLDS user accounts of former and transferred employees are timely deactivated, and the TFA tokens are timely retrieved by the PDPA who will immediately deactivate the user's access, and request the return of the token from the employee's supervisor. Either deactivation or retrieval of the token will signify that access has been terminated. In circumstances relating to employee transfers, the PDPA inquires with the new supervisor to determine if NSLDS access is still needed. If so, access is retained and documented. If continued access is no longer required, the employee's access and NSLDS tokens are deactivated and the return of tokens is requested.

OSFA instituted additional procedures, effective April 2017, to ensure copies of emails, confirmations and screenshots are taken by the PDPA and maintained in a shared folder for tracking/auditing purposes.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.

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 as of March 28, 2018: 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.

Response as of September 30, 2018: OSFA has enhanced controls, procedures and processes ensuring that effective monthly access reviews of NSLDS user access privileges are conducted and that monitoring of NSLDS user access activity is documented. As of April 2017, these enhanced controls, procedures and processes include, creating and requesting reports at the beginning of each month, that are maintained in a shared drive for auditing/tracking purposes. Additionally, confirmation of user access is requested on an annual basis from each supervisor and documented. This confirmation procedure was updated to require the confirmation of access privileges be given only in writing (including email), effective November 2017.

Anticipated Completion Date & Contact: Complete; Martha K. Asbury and Miki Presley.