FLORIDA DEPARTMENT OF EDUCATION

Eric J. Smith
Commissioner of Education

Just Read, Florida!

January 10, 2011

Commissioner Eric J. Smith
Florida Department of Education
325 West Gaines Street, Suite 1514
Tallahassee, Florida 32399-0400

Dear Commissioner Smith:

In accordance with Section 20.055(5)(h), Florida Statutes, I am submitting the six month follow-up response concerning the Auditor General Audit report on *Information Technology Operational Audit of the Department of Education Federal Family Education Loan Program(FELP) System* for the period of July 2009 through March 2010, for your information.

If you have any questions, please contact me at 245-9418.

Sincerely,

Ed W. Jordan

Ed W. Jordan

dm/
Attachment

RECEIVED
JAN 13 2011

cc: Linda Champion, Deputy Commissioner
Levis Hughes, Office of Student Financial Assistance
David Martin, Auditor General
Florida Joint Legislative Auditing Committee

	Information Technology Operational Audit of the FFELP System	
	for the period of 7/2009 through 3/2010	
	Status of Actions taken due by Dec. 29, 2010	
		Status as of 12/29/2010
Finding No. 1: Security Administration Procedures	Finding: The Department's security administration procedures did not address some important aspects of mainframe user account management.	
	Recommendation: The Department should enhance its security administration procedures by documenting management's expectations for managing mainframe user accounts.	
1.1	Specific security administrator steps in creating or disabling user accounts, including which screens are to be used, how login identification codes (IDs) are to be assigned, and specific user account parameters that must be set.	Complete. Security administration steps have been documented and included within the security administrators' procedures.
1.2	Descriptions of userID string types (naming conventions) and how they should be assigned to users (e.g., based on least privileges required for job position and duties).	Complete. UserID string types have been documented.
1.3	Management of access rules that define access privileges to specific data sets.	To be complete by 1/20/11. Access rules have been fully reviewed and documented. We will update the rules to eliminate terminated employees.
Finding No. 2: Appropriateness of Access Privileges	Finding: Some unnecessary or inappropriate mainframe and FFELP system access privileges existed among OSFA, financial institution, and educational entity staff. Department management did not periodically review the appropriateness of mainframe FFELP System access privileges.	
	Recommendation: The Department should ensure that mainframe and FFELP System access privileges are appropriately restricted to only what is needed for users to perform their assigned job duties. Additionally, the Department should periodically review active mainframe and FFELP System user accounts to identify and adjust any inappropriate or excessive access privileges.	Monitoring reports are now created and reviewed at least once monthly to ensure ongoing appropriate access is granted. A user access request form has been implemented to ensure more timely access and suspension of user accounts.

	Information Technology Operational Audit of the FFELP System for the period of 7/2009 through 3/2010 Status of Actions taken due by Dec. 29, 2010	
		Status as of 12/29/2010
2.1	The test of 128 active mainframe user accounts in the OSFA FFELP user and IT user groups as of 12/7/09 identified 33 user accounts that were unnecessary or that had access privileges that were inappropriate for the employees to whom they wer assigned. Of the 33 accounts, 9 had never been used	Complete. A full user report was produced, and all user accounts, including the 33 sampled, that had not been accessed for more than 90 days were suspended.
2.2	The test of 128 active mainframe user accounts in the OSFA FFELP user and IT user groups as of 12/7/09, identified 33 user accounts that were unnecessary or that had access privileges that were inappropriate for the employees to whom they were assigned. Of the 33 accounts, 10 had not been used for 203 to 3558 days	Complete. A full user report was produced, and all user accounts, including the 33 sampled, that had not been accessed for more than 90 days were suspended.
2.3	The test of 128 active mainframe user accounts in the OSFA FFELP user and IT user groups as of 12/7/09, identified 33 user accounts that were unnecessary or that had access privileges that were inappropriate for the employees to whom they were assigned. Of the 33 accounts, 15 had TSO or JOB privileges that were not necessary for the employees' job duties	Complete. A full user report was produced, and all user accounts, including the 33 sampled, were suspended or changed to minimize access to the current need.
2.4	The test of 128 active mainframe user accounts in the OSFA FFELP user and IT user groups as of 12/7/09, identified 33 user accounts that were unnecessary or that had access privileges that were inappropriate for the employees to whom they were assigned. Of the 33 accounts, 7 had inappropriate userID string assignments	To be complete by 1/20/11. A full user report was produced, and all user accounts, including the 33 sampled, are being compared with the analysis of userID strings. UserIDs will be reassigned as appropriate.
2.5	The test of 333 active mainframe user accounts in the financial institution and education entities user groups as of 12/7/09 identified 311 user accounts that were unnecessary or that had access privileges that were inappropriate for the employees to whom they were assigned. Of the 311 user accounts: 193 had never been used.	Complete. A full user report was produced, and all user accounts, including the 333 sampled, that had not been accessed for more than 90 days were suspended.
2.6	The test of 333 active mainframe user accounts in the financial institution and education entities user groups as of 12/7/09 identified 311 user accounts that were unnecessary of that had access priviletges that were inappropriate for the employees to whom they were assigned. Of the 311 user accounts: 105 had not been used for 161 to 3875 days	Complete. A full user report was produced, and all user accounts, including the 333 sampled, were suspended that had not been accessed for more than 90 days.

	Information Technology Operational Audit of the FFELP System	
	for the period of 7/2009 through 3/2010	
	Status of Actions taken due by Dec. 29, 2010	
		Status as of 12/29/2010
2.7	The test of 333 active mainframe user accounts in the financial institution and education entities user groups as of 12/7/09 identified 311 user accounts that were unnecessary of that had access priviletges that were inappropriate for the employees to whom they were assigned. Of the 311 user accounts: 10 had TSO or JOB privileges that were not necessary for the employee's job duties.	Complete. A full user report was produced, and all user accounts, including the 333 sampled, were reviewed to ensure TSO, JOB, and CICS were appropriately assigned, and modified where appropriate.
2.8	The test of 333 active mainframe user accounts in the financial institution and education entities user groups as of 12/7/09 identified 311 user accounts that were unnecessary of that had access priviletges that were inappropriate for the employees to whom they were assigned. Of the 311 user accounts: 16 had inappropriate user ID string assignments.	To be complete by 1/20/11. A full user report was produced, and all user accounts, including the 33 sampled, are being compared with the analysis of userID strings. UserIDs will be reassigned as appropriate.
2.9	The sample of 35 active FFELP System user accounts identified 5 instances of unnecessary or inappropriate access. 2 FFELP user accounts assigned to one OSFA employee included unnecessary security administration access privileges, increasing the risk that the privileges will be misused.	Complete. Security administration access privileges are now assigned only to one primary security administrator, and 3 backups. This will be reduced to 2 backups once all training is complete.
2.10	The sample of 35 active FFELP System user accounts identified 5 instances of unnecessary or inappropriate access. 2 OSFA employees with programming access privileges also had access privileges that included security administration capabilities, contrary to an appropriate separation of duties.	Complete. The designated new primary, and first backup, security administrators do not have programming access privileges. The second backup has programming privileges, but only performs these activities in an emergency in the absence of the first 2 people. There are no other non-programming staff available.
2.11	The sample of 35 active FFELP System user accounts identified 5 instances of unnecessary or inappropriate access. 1 OSFA employee with programming access privileges also had update access to the FFELP System in production, contrary to an appropriate separation of duties.	Complete. Access for the programmer was changed to inquiry only, and all other programmers access was reviewed.

	Information Technology Operational Audit of the FFELP System for the period of 7/2009 through 3/2010 Status of Actions taken due by Dec. 29, 2010	Status as of 12/29/2010
Finding No. 3: Timely Disabling of Former Employee Access	Finding: The Department lacked written procedures for the disabling of IT access privileges for former employees and did not disable the access privileges of some former OSFA employees in a timely manner. In addition, contrary to the requirements of the Department of State General Records Schedule for retention of access control records, the Department did not retain FFELP System access control records of former employees.	
	Recommendation: The Department should establish written procedures for the timely disabling of former OSFA employee access privileges and retain access control records for the FFELP System in accordance with the requirements of the General Records Schedule.	
3.1	Establish written procedures for the timely disabling of former OSFA employees access privileges.	Complete. Disabling system access is part of the OSFA employee termination process. Procedures have been reviewed, and a new security access request form has been implemented.
3.2	Retain access control records for the FFELP System in accordance with the requirements of the General Records Schedule.	Complete. General Records Schedule provides that access control records must be retained for one year after the employee separates from employment. NWRDC does not provide the facility for this data retention. The associated risk is mitigated by ensuring last access dates are reviewed on monitoring reports, and UserIDs are not reused.
Finding No. 4: Unique User Identification	Some temporary OSFA staff shared generic user identifications (IDs) for FFELP System access that may have limited the Department's ability to establish accountability for FFELP System actions.	
	Recommendation: The Department should assign unique login IDs to all individual users authorized to access the NWRDC mainframe and the FFELP System.	

	Information Technology Operational Audit of the FFELP System for the period of 7/2009 through 3/2010 Status of Actions taken due by Dec. 29, 2010	Status as of 12/29/2010
4.1	Assign unique login IDs to all individual users authorized to access the NWRDC mainframe and the FFELP System.	Complete. Unique login IDs have been assigned to all individual users of the NWRDC mainframe and FFELP system. Ongoing creation and suspension of accounts will be requested via the security access request form.
Finding No. 5: User Authentication	Finding: Certain Department security controls related to user authentication needed improvement.	
Note: Finding 5 is considered CONFIDENTIAL.	Recommendation: The Department should improve security controls related to user authentication to ensure the confidentiality, integrity, and availability of Department data and IT resources.	
5.1	Network password controls were set to allow up to 10 invalid logon attempts and to reset the account after 2 minutes. Change to lock after 5 unsuccessful logon attempts and be reset either by Help Desk staff or automatically after 5 minutes.	Complete. Network account locks after 5 unsuccessful logon attempts, and is reset either by help desk staff or automatically after 5 minutes.
5.2	The minimum network password age (number of days that a password must be used before user can change it) was set to zero days and the password history (number of passwords that are stored in history and cannot be used) was set to one for the network. Change network password settings according to DOE policy.	Complete. Number of days has been set to 28-35 days, and password history has been set to 3. This aligns with DOE policy.
5.3	Mainframe ACF2 password settings allowed for a minimum password length of 6 characters, passwords were not required to be changed, and the settings did not prevent the reuse of passwords. Change to require a minimum password length of 8 characters, require passwords to be changed at specific intervals, and prevent the immediate reuse of the same password.	Complete. ACF2 password length is a constraint of NWRDC and cannot be changed for DOE only. Intervals of password changes have been set to 28-35 days. Password history retention is a system-wide function, thus NWRDC could not set password history retention for DOE only. NWRDC indicates they will continue to analyze this need. Currently ACF2 users cannot repeat a password immediately, but can repeat a password after 1 28 to 35 day cycle.

	Information Technology Operational Audit of the FFELP System for the period of 7/2009 through 3/2010 Status of Actions taken due by Dec. 29, 2010	Status as of 12/29/2010
5.4	The FFELP System minimum password length is set to 3 characters, does not require complex passwords, stored passwords in clear text, did not maintain a history of passwords, and allowed the passwords to be changed within the same day. Change the system to comply with Department's End User Best Practices documentation which specifies a minimum password length of 8 characters, composed of 3 of the following: uppercase letters, lowercase letters, numerals, and special characters; encrypted passwords, maintaining a password history of 3 previous passwords; and that previous passwords need to be used for at least 30 days.	Complete. The FFELP application system pasword characteristics have not been changed. OSFA is willing to accept any associated risk, and monitors system access regularly. This modification would be a substantial system change, which will be addressed by OSFA in it's strategic business planning in determining how long this system will remain on the mainframe.
5.5	ACF2 provides settings to control inactive Customer Information Control System (CICS) and Time Sharing Option (TSO) sessions. These settings provide the ability to limit the amount of time a CICS or TSO session can remain active when not in use and are applied on a user-by-user basis. None of the 388 CICS user accounts had the ACF2 CICS time-out setting in place, and 200 or the 253 user accounts with TSO privileges did not have the TSO time-out setting in place. In addition, the FFELP System does not require users to log on the system after a designated period of inactivity. Department End User Best Practices required that unattended sessions be locked and require a password to regain access. Change CICS and TSO settings to comply; and change the FFELP System to require users to log on after a periopd of inactivity.	Complete. CICS and TSO timeout settings have been implemented for all system users and programmers at 30 minutes of inactivity.
Finding No. 6: Program Change Controls	Finding: The Department had not established a written System Development Life Cycle methodology to govern the development and modification of its application systems. In addition, existing OSFA written procedures did not address certain important aspects of the program chasnge process for the FFELP System.	
	Recommendation: The Department should establish a written Departmentwide System Development Life Cycle methodology that provides the minimum expectations for controlling the development and modification of all Department application systems and establish more comprehensive FFELP System program change control procedures to provide increased assurance that only authorized programs and program changes are implemented into the FFELP System.	

	Information Technology Operational Audit of the FFELP System for the period of 7/2009 through 3/2010 Status of Actions taken due by Dec. 29, 2010	Status as of 12/29/2010
6.1	The Department had not estblished a written Departmentwide System Development Life Cycle methodology to govern the development and modification of its application systems. In addition, existing written OSFA procedures did not address the following important aspects of the program change process for the FFELP System: The employees who may authorize a change and how authorizations are to be documented. Modify the SRS to ensure proper documentation, and/or develop hardcopy forms.	Complete. The Information System Development Methodology (ISDM) has been implemented for OSFA projects, and is under executive review for DOE-wide implementation. In addition, the OSFA Service Request System has been modified to require electronic signature authroizing programming change requests, and authorizing new programming to be moved to a production environment.
6.2	The Department had not estblished a written Departmentwide System Development Life Cycle methodology to govern the development and modification of its application systems. In addition, existing written OSFA procedures did not address the following important aspects of the program change process for the FFELP System: How changes will be tested. Modify the SRS to ensure proper documentation, and/or develop hardcopy forms.	Complete. The Information System Development Methodology (ISDM) has been implemented for OSFA projects, and is under executive review for DOE-wide implementation. In addition, the OSFA Service Request System has been modified to require electronic signature authorizing programming change requests, tracking user acceptance testing, and authorizing new programming to be moved to a production environment.

	Information Technology Operational Audit of the FFELP System for the period of 7/2009 through 3/2010 Status of Actions taken due by Dec. 29, 2010	Status as of 12/29/2010
6.3	The Department had not estblished a written Departmentwide System Development Life Cycle methodology to govern the development and modification of its application systems. In addition, existing written OSFA procedures did not address the following important aspects of the program change process for the FFELP System: The employees who may approve the implementation of program changes. Modify the SRS to ensure proper documentation, and/or develop hardcopy forms.	Complete. The Information System Development Methodology (ISDM) has been implemented for OSFA projects, and is under executive review for DOE-wide implementation. In addition, the OSFA Service Request System has been modified to require electronic signature authorizing programming change requests, tracking user acceptance testing, and authorizing new programming to be moved to a production environment, based on predetermined role assignment.
6.4	The Department had not estblished a written Departmentwide System Development Life Cycle methodology to govern the development and modification of its application systems. In addition, existing written OSFA procedures did not address the following important aspects of the program change process for the FFELP System: The employees who may implement the program changes into the production environment. Change the production move process, specifically who performs production moves, and a way to ensure complete documentation is present for all system changes.	Complete. A person without programming access permissions has been assigned and trained to perform production moves. This person will ensure the presence of complete documentation for each production move as part of their duties. One non-programmer person is assigned to function as backup for moving web pages, and 2 people are assigned as backup for moving mainframe code.