FLORIDA DEPARTMENT OF EDUCATION

December 14, 2009

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

Dear Commissioner Smith:

The attached six month follow-up to the Auditor General's report 2009-208 regarding *Department of Education, Rehabilitation Information Management System (RIMS) and Accessible Web-Based Activity and Reporting Environment (AWARE)* is for your information. Actions taken by Department offices have addressed all recommendations of the Auditor General.

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

Sincerely,

Ed W. Jordan

Ed W. Jordan
/br
Attachment
c: Auditor General
Florida Joint Legislative Auditing Committee
Linda Champion
Martha Asbury

RECEIVED
DEC 18 2009

Florida Department of Education
Auditor General Report 2009-208
6 Month Follow-up RIMS/AWARE Response
12/7/2009

Six-Month Update: **As appropriate, the six month updates provided below, specifically reference the Division of Vocational Rehabilitation and the Division of Blind Services; however, all actions have been taken in conjunction with the Department's Chief Information Officer and the Office of Technology and Information Services.**

Finding 1
The placement of the Chief Information Officer (CIO) within the Department's organizational structure and the scope of his authority for performing IT duties assigned in State law needed improvement to provide increased authority over all Department IT functions.

RESPONSE:
The Department has determined that the Office of Technology and Information Services (OTIS) and the Chief Information Officer (CIO) are correctly placed organizationally within the Division of Finance and Operations, reporting to the Deputy Commissioner for Finance and Operations. It is not correct that placement within this Division resulted in the CIO's focus being on IT management only for the Division. The OTIS provides IT management for all divisions within the Department. The Division of Finance and Operations was established for the purpose of providing infrastructure support for the Department. Therefore, it is completely appropriate for an infrastructure function such as IT to reside within the Division. This purpose is evidenced by other organizational units within the Division of Finance and Operations. For example, the Bureau of Contracts, Grants, and Procurement and the Bureau of Personnel Management and Labor Relations reside in the Division of Finance and Operations and provide services, support, and oversight (as appropriate) to the entire Department. In every instance, infrastructure support from these Department-wide functions is equitably distributed among all of the organizational entities within the Department and resources are allocated based upon identified needs. Documentation of services, support, and oversight provided across the Department can be provided upon request.

The Department has taken steps to redefine current responsibilities of OTIS and the CIO to include oversight of all IT operations within the Department, including IT operations now being managed separately by DVR and DBS.

The Department's previous comment to this finding remains unchanged.

Finding 2
The Department, DVR, and DBS had not clearly established the roles and responsibilities of the Department's Information Security Manager (ISM) and the Division data security administrators.

RESPONSE
The Department has clearly established the roles for the Information Security Manager and Information Security Officer. These roles and responsibilities are stated in revised position descriptions and work plans. DVR and DBS are currently working with the CIO to align roles and responsibilities of staff members assigned to security functions.

The Department's previous comment to this finding remains unchanged.

Finding 3
The Department's security program, including its security policies and procedures, needed improvement.

RESPONSE
The Department's security program policies and procedures have been revised and updated and are currently undergoing final review prior to approval. The policies and procedures were written to be consistent with the Office of Information Security's efforts to create a statewide policy standard for Florida State Government and are inclusive of input from all affected parties. Additionally, the Department's internal operating procedures (IOPs) are undergoing regularly scheduled review and updating and will be revised as necessary to reflect the content of the security program policies and procedures. Again, these IOPs are designed to apply to the entire Department, including the Divisions of Vocational Rehabilitation and Blind Services.

DBS has contracted with Dyntek to facilitate the development of a security program, policies, procedures, and plan. The deliverables will include network and firewall policies, application change management, disaster recovery, access control, password, data classification, and other applicable security policies.

Finding 4
The Department had not prepared security plans and strategies for implementing appropriate cost-effective safeguards to reduce, eliminate, or recover from the identified risks to data, information, and IT resources.

RESPONSE
The Department has written and submitted for approval, a comprehensive strategic security plan and an annual security work plan for 2009. The security work plan was designed to address the findings in the DOE 2008 Risk Assessment.

Additionally, the DBS conducted a Security Assessment based on International Organization for Standardization (ISO) 17799, Rule 60-DD, and the Auditor General's AWARE audit. The DBS is developing an IT security plan to address risks found in the assessment.

Finding 5
Although new employees received security awareness orientation and the Department had security awareness training materials available for all employees, training was not provided on a recurring basis. In addition, the Department did not retain documentation of employee participation in security awareness training activities.

RESPONSE
Plans are in development to create an in-house web based application to track on-going Information Security Awareness Training for all Department employees and contracted staff. This training is intended to be recurring on an annual basis.

While the Department is developing an in-house Web based application to track on-going Information Security Awareness, this project is in the planning phase. Training will be provided to all Department and contracted staff and will continue to occur on an annual basis.

Finding 6
The Department did not have a Department-wide disaster recovery plan that included procedures for annual testing and applied to all critical Department IT resources.

RESPONSE
The Department's disaster recovery plan will be amended to include all critical IT resources, including DVR and DBS resources. All elements of the plan will be tested annually.

The elements of the Department's disaster recovery plan are tested annually. The disaster recovery plans for the DVR and DBS will include a review by the Department's CIO to ensure that all of the Department's critical IT resources ensure a prompt and effective continuation of services.

Finding 7
The Department did not perform Federal background checks on DVR RIMS application contractors. Department policies contained inconsistent guidance regarding whether contractors could be considered as working in positions of special trust.

RESPONSE
The Department's internal operating procedures (IOPs) are undergoing regularly scheduled review and updating and will be revised as necessary to clarify the inclusion of contractors as positions of special trust. Contractors working on the RIMS application are currently undergoing Level I background screening.

The Department's previous comment to this finding remains unchanged.

Finding 8
Security administration procedures needed improvement.

RESPONSE

The Department is contracting with a vendor to assist with creating an on-line tracking and auditing system for establishing and deleting user access to the DBS network and AWARE system. The on-line tracking and auditing system will be completed by December 31, 2009. The DVR has acquired the missing user forms referenced in the report. The Department is also revising the DVR procedures for establishing and removing access privileges.

The DVR has revised the procedures for establishing and removing access privileges for RIMS. Appropriate staff have been trained on and provided with the revised procedures.

The DBS has engaged a consultant to facilitate development of an IT security program, policies, procedures, and plan. Security administration procedures will consist of documentation of access controls such as authentication controls, a password policy and technical controls, and authorization controls based on data classification.

Specifically, DBS is in the process of developing written procedures for AWARE and DBS network security administration. The AWARE and DBS network security administration procedures will delineate who can approve access, establish periodic review of access privileges by management, and retention of records documenting approval of access.

The DBS put the approved password policy into effect for the DBS network and AWARE on December 2, 2009. The data classification policy has been drafted and is expected to be in place by December

31, 2009. A review/reconciliation of access privileges, including written authorizations, will be conducted by March 2010. The policies and procedures to fully implement proper authorization, management review, and record retention of approval records will be in place by March 2010.

Finding 9
Some access capabilities relating to RIMS, AWARE, and the surrounding IT infrastructure did not enforce an appropriate separation of incompatible duties or were excessive.

RESPONSE

The DBS has conducted an assessment of roles and responsibilities related to AWARE and access rights of IT staff assigned specific roles within the system.

A separation of duties with a small staff (6 FTE and 3 contractors) is difficult. DBS staff are required to perform duties related to application code development, code promotion to production, DBS network administration, database administration, AWARE account administration, and AWARE support. However, each of the above roles has been documented. A matrix will be developed with separation of duties and access will be administered based on the matrix. Access rights for administrative roles related to the DBS network and AWARE will be reviewed periodically – at least annually.

The DVR is in process of developing a matrix identifying the separation of duties and access. Separation of duties will be administered based on the matrix. Access rights for administrative roles related to the DVR network and RIMS will be reviewed annually. The anticipated date for full implementation is April 30, 2010.

Finding 10
Access privileges, in some instances, were not timely removed or revoked for former employees and contractors.

RESPONSE

The Department is contracting with a vendor to assist with creating an on-line tracking and auditing system for establishing and deleting user access to the DBS network and AWARE system. The on-line tracking and auditing system will be completed by December 31, 2009. With respect to DVR, old accounts have been removed and a procedure has been developed to review network accounts for inactivity on a weekly basis.

The DBS is implementing a series of controls to minimize the chance for recurrence of former employees and contractors retaining access privileges after termination of employment. For example, the DBS is in the process of developing an access control policy which includes immediate revocation of access upon termination of employment or contract status. Additionally, the DBS is implementing a process to determine current employee accounts which have not logged on to the DBS network within the past 30-60 days to assess continued need for access.

The DVR has removed all old accounts and a new procedure for reviewing inactivity of network accounts is being maintained weekly.

Finding 11
Certain security controls related to DVR and DBS and AWARE, needed improvement, in addition to the matters discussed.

RESPONSE
The Department has noted this finding and will continue to address continued improvements in security controls.

The Department's previous comment to this finding remains unchanged.

Finding 12
Contrary to Section 119.071(5)(a)2.a., Florida Statutes, employee social security numbers (SSNs) without specific authorization established the imperative need to use the SSN for the performance prescribed by law.

RESPONSE
The Department is no longer using employee social security numbers in RIMS.

No further action is necessary.

Finding 13
The environmental controls in the DVR and DBS respectively, were deficient.

RESPONSE
The Department will implement additional controls to protect computer equipment from environmental hazards, to the extent that fiscal resources are available to do so. The DBS data center services and network hardware have been relocated to the DOE Data Center as of April 25, 2009. The DOE Data Center is climate controlled. In the event of an emergency situation, the DOE Data Center is adequately equipped to mitigate damage or failure.

No further action is necessary.

Finding 14
The Department had inadequate controls over RIMS and AWARE.

RESPONSE
The Department's OTIS is working closely with DVR and DBS staff to ensure that program change control practices and procedures are revised as necessary to provide enhanced security and consistency across the Department. Written program change control procedures will be enhanced.

The Department's previous comment to this finding remains unchanged.

Finding 15
DVR customer service information in RIMS was not being entered into RIMS. This omission diminished the completeness and the reliability and usefulness of reports generated from RIMS.

RESPONSE

The Department is taking steps to ensure that all DVR customer services are entered into RIMS.

The DVR has made necessary changes within RIMS to accommodate the addition of the outstanding contracts for customer services in order to accurately track the services. All of the outstanding contracts have been entered into RIMS, with full ability of tracking targeted for January 2010.