REPORT NO. 2009-208
MAY 2009

# DEPARTMENT OF EDUCATION

## REHABILITATION INFORMATION MANAGEMENT SYSTEM (RIMS) AND ACCESSIBLE WEB-BASED ACTIVITY AND REPORTING ENVIRONMENT (AWARE)

Information Technology Operational Audit

August 2008 Through November 2008
and Selected Actions Through February 2009

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

## 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 of Education. Dr. Eric J. Smith served as Commissioner of Education during the audit period.

The audit team leaders were Hilda S. Morgan, CPA, CISA, and Robert McKee, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

# DEPARTMENT OF EDUCATION

## Rehabilitation Information Management System (RIMS)
## and
## Accessible Web-based Activity and Reporting Environment (AWARE)

## SUMMARY

**The Rehabilitation Information Management System (RIMS) and the Accessible Web-based Activity and Reporting Environment (AWARE) are case management systems used by the Division of Vocational Rehabilitation (DVR) and the Division of Blind Services (DBS), respectively, to manage services for individuals with disabilities through division programs that provide assistance in achieving self-sufficiency.**

**Our audit focused on evaluating the effectiveness of selected information technology (IT) controls applicable to RIMS and AWARE for the period August 2008 through November 2008 and selected actions through February 2009.**

**The results of our audit are summarized below:**

**Finding No. 1:** **The placement of the Chief Information Officer (CIO) within the Department's organizational structure needed review and the scope of his authority for performing IT duties assigned in State law needed improvement to provide increased oversight of all Department IT functions.**

**Finding No. 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.**

**Finding No. 3:** **The Department's security program, including its security policies and procedures, needed improvement.**

**Finding No. 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.**

**Finding No. 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.**

**Finding No. 6:** **The Department did not have a Departmentwide disaster recovery plan that included procedures for annual testing and applied to all critical Department IT resources.**

**Finding No. 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.**

**Finding No. 8:** **Security administration procedures needed improvement.**

**Finding No. 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.**

**Finding No. 10:** **Access privileges, in some instances, were not timely removed or revoked for former employees and contractors.**

**Finding No. 11:** **Certain security controls related to DVR and DBS data and IT resources, including RIMS and AWARE, needed improvement, in addition to the matters discussed in Finding Nos. 8 through 10.**

**Finding No. 12:** **Contrary to Section 119.071(5)(a)2.a., Florida Statutes, DVR collected and used certain employee social security numbers (SSNs) without specific authorization in law or without having established the imperative need to use the SSN for the performance of its duties and responsibilities as prescribed by law.**

**Finding No. 13:** **The environmental controls in the DVR and DBS server rooms for RIMS and AWARE, respectively, were deficient.**

**Finding No. 14:** **The Department had inadequate controls over the program change control process for RIMS and AWARE.**

**Finding No. 15:** **DVR customer service information in RIMS was incomplete because group services were not being entered into RIMS. This omission diminished the completeness of RIMS case management data and the reliability and usefulness of reports generated from RIMS.**

## BACKGROUND

The Department of Education (Department) is responsible for public education in the State of Florida under the direction of the State Board of Education, pursuant to Section 1001.20(1), Florida Statutes. Pursuant to Section 20.15(3), Florida Statutes, two of the Department's established divisions are the Division of Vocational Rehabilitation (DVR) and the Division of Blind Services (DBS).

The Department, through DVR and DBS, enhances the economic self-sufficiency of Floridians through programs and services geared toward workforce education, apprenticeships, job-specific skills, and career development. DVR and DBS manage the programs that assist individuals who are disabled or blind or visually impaired, respectively, to succeed either in the school setting or in careers, encouraging independence and self-sufficiency.

The Department maintains various computer facilities, including the Education Data Center, the DVR server room, and the DBS server room. The CIO has authority over the Education Data Center and certain other Department IT functions. However, the DVR and DBS server rooms and all related IT functions and networks are managed by their respective divisions.

RIMS is a 2-tier client system that is operated in the DVR server room. It is a case management system that is accessed through the DVR network to manage and track vocational rehabilitation services for individuals with disabilities who require vocational rehabilitation services to prepare for, secure, regain, or retain employment.

AWARE is a Web-based system that is operated in the DBS server room. It is a case management system that is accessed through the Internet by the application users to manage and track vocational rehabilitation and independent living services for individuals who are blind or visually impaired and is accessed through the DBS network for system administration.

## FINDINGS AND RECOMMENDATIONS

Our audit disclosed that IT controls and practices applicable to RIMS and AWARE needed improvement. As discussed in the Background section of this report, the Department's management of the IT infrastructure for RIMS and AWARE was decentralized, with DVR and DBS IT functions operating separate and autonomous from the authority of the Department's CIO. However, because DVR and DBS, by law, are under the direction of the Department, the Department is ultimately responsible and accountable for managing the IT resources of DVR and DBS, including, in particular, RIMS and AWARE. Accordingly, we encourage the Commissioner of Education and Department CIO to provide centralized management oversight of DVR and DBS IT operations and work with the respective Divisions to address the findings and recommendations included in this report.

## Security Management

An entitywide information security program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. An effective information security program establishes a framework and continuing cycle of activity for assessing risk, establishing entitywide security policies and plans, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures.

### Finding No. 1: IT Organizational and Management Structure

Section 282.3055, Florida Statutes, provides that an agency CIO shall be appointed and respective duties include, but are not limited to, coordinating and facilitating the planning and management of agency information technology services, implementing agency IT planning and management procedures, guidelines, and standards that are consistent with the procedures and standards adopted by the Agency for Enterprise Information Technology, advising agency senior management as to agency IT resource planning and needs, and assisting in the development and prioritization of IT resource needs for the agency's budget request. It is essential that the IT function be properly placed within the overall agency organizational structure to ensure an appropriate degree of separation from other organizational units and adequate authority to manage and provide governance for the organization's IT functions.

According to Department policies, the Department CIO is responsible for advising senior management as to the enterprise resource planning and management needs for inclusion in planning documents required by State law. The CIO is also assigned overall responsibility for developing Department IT resource policy, standards, and procedures and for coordinating the preparation of the information resource plans and reports required by State law and the administrative rules subject to the approval of the Commissioner of Education. The Department's divisions are responsible for designating representatives who will provide the information as requested by the CIO or his designee. Also, the CIO and the Office of Technology and Information Services are to provide consulting services to the divisions for IT resource acquisitions and dispositions.

Our audit disclosed that the CIO was organizationally located within the Office of Technology and Information Services and reported to the Chief Education Finance Officer in the Division of Finance and Operations. Placement within this Division did not ensure proper IT management authority and oversight of DVR and DBS by the CIO. DVR and DBS were separate divisions within the Department. DVR and DBS server rooms and related IT resources were controlled by the respective Management Information Systems (MIS) sections within their Divisions and were not under the authority of the CIO. The Department CIO did not monitor DVR or DBS IT activities or their compliance with Department IT policies.

Without appropriate CIO oversight of all IT operations within the Department, the risk is increased that Department policies and procedures, including security controls to reduce or eliminate risks to the Department, may not be followed consistently by all divisions or in a manner pursuant to management's expectations.

**Recommendation: The Department should review the organizational placement of the Office of Technology and Information Services and the CIO and redefine current responsibilities to include oversight of all IT operations within the Department, including IT operations now being managed separately by DVR and DBS, to provide increased assurance that RIMS, AWARE, and the surrounding IT infrastructure are being managed and secured according to Department IT resource policy, standards, and procedures.**

## Finding No. 2: Information Security Manager and Data Security Administrators

Pursuant to Section 282.318(2)(a)1., Florida Statutes, each agency head is responsible for designating an Information Security Manager (ISM) to administer the security program of the agency for its data and IT resources. The duties of the ISM include performing agency risk assessments; developing policies and procedures that include an incident management program when a security incident or data compromise occurs; documenting in security plans and strategies the use and implementation of cost-effective controls to reduce, eliminate, or recover from identified risks; ensuring that internal self-assessments or audits of the agency security program are conducted; and including security requirements within specifications when soliciting use of third-party resources. Pursuant to Department of Management Services Rule 60DD-2.001(2)(a)34., Florida Administrative Code, the Department may designate a number of data security administrators to monitor and implement security controls and procedures for a system. Therefore, it is essential that the responsibilities and roles of the ISM and the data security administrators are clearly defined.

Although the Commissioner of Education had designated an ISM, the Department had not adequately defined and documented the roles and responsibilities for the ISM and data security administrators. The ISM position reported directly to the CIO with a position title of Operations and Management Consultant Manager. However, the job description for this position did not include the responsibilities of the Department ISM. Additionally, DVR and DBS had not documented the roles and responsibilities of their data security administrators for securing their respective networks and applications.

Without clearly defining and documenting the roles and responsibilities of the Department ISM and DVR and DBS data security administrators, the risk is increased that management's expectations for implementing security controls for maintenance of data and information resource confidentiality, integrity, and availability may not be consistently met.

**Recommendation: The Department should define and document the roles and responsibilities of the Department ISM and DVR and DBS data security administrators.**

## Finding No. 3: Security Program Policies and Procedures

Effective security management includes the development of entitywide security policies and plans, along with system- and application-specific procedures to implement the entitywide policies. The Department had policies addressing security program requirements  but had not developed procedures to implement the policies. Based on the IT organizational structure of the Department, the MIS sections of DVR and DBS each maintained their IT services independent of the Department CIO.

Our review of the Department security policies disclosed that the policies:

- Were not current. For example, the policies referred to the State Technology Office, which has not existed since July 2005, rather than the Agency for Enterprise Information Technology, which was created in State law in July 2007 as the replacement for the State Technology Office.
- Did not address network and firewall security.
- Did not suitably address IT disaster recovery planning. The policies addressed backup and recovery responsibilities, but IT disaster recovery planning also involves such activities as alternate processing sites, priorities for restoring applications, critical contact list of employees and vendors, and annual testing of the plan. None of these activities were addressed in policy.

- Did not suitably address application change management. Responsibilities for project changes were addressed, but application change management activities also include authorization, user acceptance testing, movement of programs into production, and adequate documentation of each step in the process. None of these activities were addressed in policy.
- Individually lacked effective, revision, or approval dates.

According to Division management, DVR and DBS generally relied on the Department policies. DVR maintained minimal policies and procedures related to the Division and RIMS. DBS had developed an additional policy related to AWARE change management. However, neither DVR nor DBS had fully developed procedures to implement Department policies. In response to audit inquiry, DBS staff stated that they were unaware of some applicable Department policies, such as incident response, access procedures, and monitoring. Without up-to-date, complete, and approved policies and procedures, the risk is increased that IT security controls may not be followed consistently across all divisions and in a manner pursuant to management's expectations.

**Recommendation: To improve the security program in the area of security planning and management, the Department and divisions should work together to fully develop, officially approve, implement, and keep current, as applicable, appropriate security program policies and procedures to maintain data confidentiality, integrity, and availability.**

## Finding No. 4: Security Plans and Strategies

An IT security plan is a written plan that provides an overview of the IT security requirements and describes the controls in place or planned for meeting those requirements. Pursuant to Section 282.318(2)(a)4., Florida Statutes, agencies are required to implement cost-effective safeguards to reduce, eliminate, or recover from the identified risks to the data, information, and IT resources of the agency. The security plan should document the cost-effective safeguards used that have been identified through risk analysis. The purpose of the plan is to protect the confidentiality, integrity, and availability of agency IT resources.

The Department, using DynTek services, performed a risk analysis in December 2005, as required by Section 282.318(2)(a)2., Florida Statutes. The Department did not include RIMS or AWARE as critical systems in the risk analysis but did include other DVR and DBS systems. Although AWARE was not included in the Department's risk analysis, DBS separately contracted with DynTek to perform security assessments in 2006 and 2007 to evaluate the external IT environment of the DBS network that supports AWARE.

Although the Department had performed a risk analysis and DBS had performed security assessments, neither had prepared a security plan or strategies to document the controls implemented or planned for implementation to protect the confidentiality, integrity, and availability of Department data and information resources. DVR had developed an action plan to address the risks identified in the risk analysis for its application, but neither the Department nor DBS had developed a security or action plan to address the risks identified in the risk analysis or the security assessments.

The absence of security plans and strategies to document the controls implemented or planned for implementation for meeting, reducing, eliminating, or recovering from the identified risks to data, information, and IT resources of the Department increases the risk that adequate security controls will not be implemented to protect the confidentiality, integrity, and availability of the data and IT resources of the Department.

**Recommendation: The Department should prepare security plans and strategies to document security controls planned or implemented to mitigate identified system security risks.**

### Finding No. 5: Security Awareness Training

A key aspect of an information security program is an ongoing security awareness training program that apprises new employees and reemphasizes to current employees the importance of preserving the security of the data and IT resources with which they are entrusted. The Department had security awareness training materials available for all employees that included special lunch and learn sessions, Gigabyte newsletter and Connections magazine articles, and best practices listed on the Department's intranet. However, the Department did not require ongoing security awareness training for its employees. New employees received security awareness orientation, but training was not provided on a recurring basis. In addition, the Department did not retain documentation of employee participation in security awareness training activities.

The lack of required and documented ongoing security awareness training limits management's assurance that employees understand the importance of IT security and are sufficiently prepared to safeguard data and IT resources.

**Recommendation: The Department should require all employees to participate in ongoing security awareness training in order to promote appropriate security practices by all employees. The Department should also retain documentation of employee participation in security awareness training activities.**

### Finding No. 6: Disaster Recovery Plans

A written, cost-effective, and tested disaster recovery plan provides for the prompt and effective continuation of State services that are critical to the continuity of governmental operations. Although the Department had developed disaster recovery plans for the Education Data Center and certain other Department IT functions, the disaster recovery plans did not specifically include the RIMS or AWARE applications or include the disaster recovery plans of DVR and DBS by reference. DVR had not developed a disaster recovery plan for its information resources, including RIMS. Conversely, DBS had developed a separate Division disaster recovery plan that included the AWARE application, but the plan had not been tested. Without documented and tested disaster recovery plans, the risk is increased that DVR and DBS may not be able to recover in a timely manner from a major disruption to their IT services.

**Recommendation: The Department should develop a Departmentwide disaster recovery plan that includes procedures for annual testing. The disaster recovery plan should include all critical Department IT resources, including DVR and DBS IT resources, either explicitly or by reference.**

### Finding No. 7: Positions of Special Trust

Section 110.1127(1), Florida Statutes, provides that each employing agency shall designate those employee positions that, because of the special trust or responsibility or sensitive location of those positions, require that persons occupying those positions be subject to a security background check, including fingerprinting, as a condition of employment. Section 435.04(1), Florida Statutes, provides that all employees in positions designated by law as positions of trust or responsibility shall be required to undergo security background investigations, referred to as level 2 background screenings, as a condition of employment and continued employment. Section 413.011(7), Florida Statutes, specifically requires that employees and applicants for employment in DBS undergo level 2 background screenings. The level 2 background screenings are to include fingerprinting for all purposes, Statewide criminal and juvenile records checks through the Florida Department of Law Enforcement, and Federal criminal records checks through the Federal Bureau of Investigation. In addition, Department of Management Services Rule 60DD-2.008(2)(c), Florida Administrative Code, provides that background investigations are required for personnel in positions of special trust or for those having access to sensitive locations, which could include contractors.

As of May 2008, the Department implemented Policy Number 18, Employment Screening, which designated all positions in the Department as positions of special trust and required background investigations pursuant to Chapter 435, Florida Statutes, and Section 110.1127(1), Florida Statutes. Pursuant to this Policy, the Department was in the process of performing level 2 background screenings for all Department employees. The Department did not, however, require a level 2 background screening for contractors. Consequently, background screenings were not being performed for DVR contractors who supported the RIMS application. DBS did require its contractors to be subject to level 2 background screenings.

Also, Policy Number 2.6, Network Security, and Policy Number 18, Employment Screening, contained inconsistent guidance regarding who is actually considered as being in a position of special trust. Policy Number 2.6 refers to IT positions as positions of special trust and refers to workers in those positions. Workers may be employees or contractors. Policy Number 18 only refers to employees and applicants for employment as requiring a level 2 background screening.

By not ensuring that contractors are included among the persons classified in positions of special trust, the risk is increased that a person with an inappropriate background could be provided access to and misuse critical IT resources.

**Recommendation: The Department should clarify its policies to include contractors in the definition of positions of special trust; take measures to ensure that contractors are appropriately and consistently classified in positions of special trust, where applicable; and ensure that all contractors in such positions receive the level 2 background screenings as required.**

## Security Controls and Other IT General Controls

### Finding No. 8: Security Administration Procedures

Security administration procedures help ensure that appropriate access controls are in place. Access controls are intended to prevent or detect inappropriate access to computer resources. Logical access controls include authentication controls, such as passwords, and authorization controls, such as access privileges. Consistent and effective management controls require documented procedures and periodic reviews of access privilege. Also, effective access controls include maintaining access authorization forms that provide documentation of appropriate approval for the access requested.

The Department did not retain access authorization documentation of the DVR network or RIMS application access privileges of DVR end users. DVR maintained a Field Services Operating Procedure, FSOP: MIS-2, Management Information System Access, revised March 2004, that specified the procedures used for requesting access and notifying MIS staff of the resignation, termination, or change in an individual's position classification. The procedure required a standardized access request form for access to the DVR network or RIMS. Of 14 IT users tested, DVR was unable to provide access authorization documentation for 8 employees and 3 contractors with access to the DVR network. Additionally, for RIMS users who must access confidential Social Security Administration information, an additional form, the State Verification and Exchange System (SVES) agreement, must be completed. However, DVR was also unable to provide access authorization documentation for 8 of 13 application users tested. In addition, 4 of 13 users did not have an SVES agreement and 2 of 13 users had agreements with missing signatures.

Also, neither the Department nor DBS had written procedures for AWARE security administration, including establishing or removing access privileges to the DBS network or the AWARE application. Documentation of approved requests for granting DBS network access privileges for system support of the AWARE application was not maintained. Additionally, procedures for user access to AWARE allowed the use of e-mail for documenting access requests. E-mails were retained as documentation of access granted since October 2006, but no documentation existed of access granted previously in the former system and imported into AWARE. Also, DBS network and AWARE application access privileges were not periodically reviewed by management. The lack of such a review may have contributed to former employees continuing to have active AWARE user accounts and user accounts having inappropriate security templates assigned (see Finding Nos. 9 and 10).

Without written procedures for establishing or removing access privileges, there is an increased risk that access controls may not be consistently applied pursuant to management's expectations. The lack of access documentation, including evidence of appropriate approval of requested access privileges, may limit management's ability to ensure the appropriateness of the access privileges to be granted. Additionally, without a periodic review of access privileges, there is an increased risk of inappropriate access privileges not being timely detected or corrected.

**Recommendation: The Department, in conjunction with DVR and DBS, should implement and maintain security administration procedures including procedures for establishing and removing access privileges, for ensuring that access documentation evidencing appropriate approval for requested access privileges to all Department's IT resources is complete, and for a periodic review of access privileges granted.**

## Finding No. 9: Separation of Duties and Excessive Access Privileges

Separation of incompatible duties is fundamental to the reliability of an agency's internal controls. An appropriate separation of duties precludes one person from controlling all steps of a process, a situation in which error or fraud could occur without timely detection. In the IT environment, examples of duties that are generally separated and assigned to individual employees or groups are changing production application programs, changing software configurations, moving programs into the production environment, and accessing production data. Effective management of user access capabilities is intended to enforce an appropriate separation of duties and ensure that users have only the access needed to perform their assigned duties.

Our audit disclosed instances of inappropriate separation of duties and excessive access privileges within DVR related to the RIMS application and administration. Specifically:

- DVR used a software contractor to perform programming and database services for the RIMS application. Contrary to an appropriate separation of duties, contractor staff had been granted read and write access to the RIMS source code and administrative privileges to the application server, database server, and RIMS database management server software. Additionally, contractor staff were provided access to move programs into the production environment. Administrative privileges provide the highest level of access granted to the network and servers, including the databases and the software running on the servers. Under these conditions, the risk was increased that unauthorized modifications to RIMS programs and data could occur and inappropriate application and database server configurations could be applied and not timely detected.

- All DVR MIS staff had been granted a user application security profile to RIMS that allowed them to perform standard MIS duties and provided them update access to the RIMS application as a user, contrary to an appropriate separation of duties.
- Certain DVR RIMS users were granted the RIMS user application security profile that provided access to confidential Social Security Administration information for DVR RIMS customers. The job classifications identified by DVR management as needing access to this data did not match the job classifications of users who had been granted this access. Although 10 job classifications were identified as needing access to the profile and the confidential data, 24 job classifications were actually granted the profile. Under these conditions, the risk was increased of unauthorized disclosure of confidential information within RIMS.

DVR management and security administrators did not conduct a periodic review of user accounts to ensure the appropriateness of access privileges. The absence of a periodic review limited DVR management's ability to timely detect excessive access privileges.

Our audit disclosed instances within DBS of inappropriate separation of duties and excessive access privileges related to the administration of the DBS network and applications and the users of the DBS AWARE application. Specifically, the administrator access group for DBS included a total of 14 individuals who had administrative privileges to the DBS network and servers, including the two AWARE servers. Administrative privileges provided the highest level of access to the DBS network and servers, including the databases and software running on the servers. Of the 14 individuals with these administrative privileges, only 5 of the individuals were responsible for supporting the AWARE infrastructure and needed administrative privileges to the AWARE servers. The other 9 individuals were either DBS employees or were contracted by DBS and supported other applications used by DBS. The two AWARE servers, the Web server, and the production server (where the database was located) were used only for the AWARE programs and data. However, all servers within the DBS network could have been accessed at the highest level by each of the individuals with administrative privileges. DBS had not established network access privileges for systems administrative staff using group access techniques to limit administrative privileges to only the devices needed to perform their specific job duties. Granting all of the DBS systems administrative staff access to the entire DBS domain at the highest privilege level increases the risk of unauthorized or erroneous disclosure, modification, or destruction of AWARE data and IT resources.

Additionally, AWARE provided user access privileges through security templates that allowed the security administrators to assign common access privileges to users who perform similar job functions. AWARE security administrators assigned security templates to users based on the users' job positions and functions. We tested all active AWARE user accounts as of October 6, 2008, with district administrator and supervisor, fiscal and budget, system administrator, program consultants, and orientation and adjustment center supervisor security templates to determine whether security templates were appropriately assigned. The system administrator template provided the highest level of access to AWARE and was to only be assigned to users who needed functionality provided by the template, such as security administrators. Our test disclosed that 5 of 49 user accounts did not have the appropriate security template assigned. Specifically:

- Two user accounts were assigned an incorrect security template based on their job positions and functions. One user should have been assigned the program consultants template instead of the system administrator template and another user should have been assigned the system administrator template instead of the program consultants template. These user accounts or user account assignments were corrected as of November 4, 2008.
- One user was assigned the program consultants template but was not in a program consultant position. Additionally, the user was not identified as a user who had permission to issue authorizations through the use of the program consultants template.

- One user account belonged to the contractor that developed AWARE. This account was assigned the system administrator template. The account was not used often and it was to only be activated when necessary and have only the minimum access capability necessary. In response to audit inquiry, DBS staff disabled this account as of October 30, 2008.
- One user account with the system administrator template belonged to a contractor in the DBS MIS section. This user did not perform security administration functions and should have been assigned a different security template.

DBS management and security administrators did not conduct a periodic review of the appropriateness of user accounts, limiting their ability to timely detect excessive access privileges. Access privileges granted in excess of what is necessary for the performance of job duties may not enforce an appropriate separation of incompatible duties and increase the risk of unauthorized disclosure, modification, or destruction of data and IT resources without timely detection.

**Recommendation: DVR should require that contractor staff maintain an appropriate separation of duties to help ensure that one individual cannot perform all job functions and should implement procedures for a periodic review of active RIMS profiles. DVR should also develop a security profile for MIS staff that prevents update access to the RIMS application. Additionally, DVR should ensure that the security profile that grants access to confidential Social Security Administration information is appropriately restricted to only the job classifications that have been determined to be in need of this level of access.**

**DBS should review its network administrative access privileges and segment the access privileges into groups that limit access by application to only those network servers and components required to support the application so that individual system administrator access is limited as needed to perform their job duties. Additionally, DBS should implement procedures for a periodic review of active AWARE user accounts and security templates to identify and adjust any inappropriate or excessive access privileges.**

## Finding No. 10: Former Employee and Contractor Access

Effective security-related policies regarding access privileges are critical to effective information system security. Effective policies include ensuring that IT management removes IT access privileges of former employees or contractors in a timely manner.

Our audit disclosed deficiencies in the timely removal of access privileges for former employees and contractors at DVR and DBS. Specifically, RIMS access privileges are granted through the use of network accounts. DVR had a Field Service Operating Procedure that addressed revocation of network accounts upon employee termination. Although the Procedure required appropriate system access changes within three days of employment termination, 3 of 197 employees who terminated employment with DVR between July 1, 2007, and October 7, 2008, continued to be defined as active in the network. Upon audit inquiry, the DVR security administrator revoked these network accounts. Under these conditions, the risk is increased of unauthorized access to RIMS data through the misuse of former employees' network accounts. The number of days between the termination dates and the dates the network accounts were revoked ranged from 34 to 235 days. One of the network accounts of a former employee had last been used 104 days after the employee's termination date. DVR staff were unable to determine what activities had been performed using the network account.

A software contractor, with an access termination request date of July 18, 2008, continued to have access to the RIMS source code library and the DVR network as of October 16, 2008. In response to audit inquiry, DVR staff removed access to the RIMS source code library on October 17, 2008. The contractor had access to the source code library 91 days beyond his access termination request date. DVR staff stated that the network account was removed between October 17, 2008, and February 17, 2009, but could not provide an exact date or supporting documentation.

AWARE access privileges are granted through the use of AWARE user accounts. DBS had undocumented procedures whereby the DBS personnel director was to notify the AWARE security administrators when employees terminated employment with DBS and, upon notification, the security administrators were to revoke former employee user accounts permitting access privileges to AWARE. However, our audit disclosed that the AWARE user accounts of 6 of 50 employees who terminated employment with DBS between July 1, 2007, and October 7, 2008, were not revoked in a timely manner. Three of the 6 former employees subsequently returned to employment. However, the elapsed time between the termination dates and the rehire dates ranged from 5 to 107 days. The remaining three former employee user accounts were revoked on October 30, 2008, in response to audit inquiry. These user accounts had access privileges to the AWARE application from 90 to 272 days after their termination dates. Our further review of active AWARE user accounts as of October 6, 2008, identified two additional user accounts that also belonged to former employees. These user accounts were revoked on November 4, 2008, in response to audit inquiry. The two user accounts had access privileges to the AWARE application or the former case management system for 584 and 2,128 days, respectively, after their termination dates. Our review of AWARE transaction logs disclosed that none of the user accounts were used after employment termination. Nevertheless, under these conditions, the risk is increased of unauthorized access to AWARE data through the misuse of former employees' user accounts.

By not removing or revoking a former employee's or contractor's network or user account that grants access to the Department's IT resources, the risk is increased that the former employee or contractor may fraudulently alter or destroy Department IT resources. Additionally, the risk is increased that current employees or contractors may access and perform unauthorized activities using the former employee's or contractor's network or user account.

**Recommendation: DVR and DBS management should ensure that network and user accounts of former employees and contractors are removed or revoked in a timely manner.**

## Finding No. 11: Other Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain DVR and DBS security controls related to RIMS and AWARE, respectively, that needed improvement, in addition to the matters discussed in Finding Nos. 8 through 10. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising DVR and DBS data and IT resources. However, we have notified appropriate Division staff of the specific issues. Without adequate security controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that DVR and DBS data and IT resources may be subject to improper disclosure, modification, or destruction.

**Recommendation: DVR and DBS should improve security controls to ensure the continued confidentiality, integrity, and availability of DVR and DBS data and IT resources.**

## Finding No. 12: Use of SSNs

Section 119.071(4)(a)1., Florida Statutes, provides that all employee SSNs held by an agency are confidential and exempt from public inspection. Pursuant to Section 119.071(5)(a)2.a., Florida Statutes, an agency may not collect an individual's SSN unless the agency has stated in writing the purpose for its collection and unless the agency is specifically authorized by law to do so or it is imperative for the performance of that agency's duties and responsibilities as prescribed by law.

DVR collected and used certain employee SSNs in RIMS. No specific authorization existed in law for DVR to collect the SSNs of RIMS users and DVR had not established the imperative need to use the SSN, rather than another number. The use of the SSN is contrary to State law and increases the risk of improper disclosure of SSNs.

**Recommendation: DVR should comply with State law by clearly establishing why the use of employee SSNs is imperative for DVR to perform its duties and responsibilities or alternatively establish another number to be used rather than the SSN.**

## Finding No. 13: Computer Facilities Environmental Controls

Environmental controls prevent or mitigate potential damage to facilities and interruption in service. Examples of environmental controls include fire extinguishers and fire suppression systems, fire alarms, smoke detectors, water detectors, backup power supplies, and shut-off valves for plumbing lines that may endanger processing facilities. Environmental controls can diminish losses or prevent incidents by detecting problems early, such as water leaks, so that they can be remedied.

Our audit disclosed environmental control deficiencies in the DVR and DBS server rooms. Specifically:

- The DVR server room did not have a raised floor. There were no water detectors and the temperature and humidity were not monitored in the room. There were three air conditioning units in the room with separate thermostats that were set and monitored manually; however, there was no automatic monitoring of the air conditioning. The air conditioning for this room was not on a separate circuit from the main power for the building. There were two fire extinguishers located in the server room; one near the front door with a last recorded maintenance date of May 2005 and one near the back door with a last recorded maintenance date of December 2000.
- The DBS server room did not have a raised floor. Although there were water sprinklers and two smoke detection sensors located in the ceiling, there were no water detectors and the temperature and humidity were not monitored by a monitoring service. There was one fire extinguisher located next to the door; however, the last recorded maintenance date of the extinguisher was May 2004.

Without adequate controls in place to safeguard computer equipment from environmental hazards, the risk is increased of equipment damage or failure in the event of an emergency situation.

**Recommendation: The Department should require DVR and DBS to establish controls to adequately protect the computer equipment from environmental hazards, including installing water detection devices, monitoring temperature and humidity, and ensuring that fire extinguishers have maintenance performed on a regular basis.**

## Finding No. 14: RIMS and AWARE Program Change Controls

Effective controls over program changes are intended to ensure that all requests for changes are standardized and subject to formal change management procedures. Program change controls include procedures to ensure that all changes are properly authorized, tested, and approved for implementation and that access to and distribution of programs are carefully controlled so that program change control activities are performed as management intended. Additionally, an appropriate separation of duties with regard to program change controls includes provisions for the movement of programs into the production environment being controlled by persons independent of the programmer making the program changes.

DVR and DBS program change controls were inadequate. Specifically:

- DVR used a work order system to track RIMS program change requests but lacked documentation of supervisory requests, programming authorization, acceptance testing, user approvals, or the movement of programs into production by the appropriate personnel. Additionally, the developers (software contractor staff) who made the program changes moved their own modified programs into the production environment, as previously discussed in Finding No. 9.
- DBS had adopted Division Policy #3.0, effective September 14, 2005, regarding the AWARE Case Management System. This Policy established the *Operational Change Management Control Procedure Manual for the AWARE Case Management System (Manual)*. However, DBS did not use the *Manual* to guide IT staff in managing AWARE program changes. Informal program change practices followed by DBS IT staff lacked documentation to demonstrate that program changes were properly authorized, tested, and approved for implementation. In addition, the movement of programs and data among libraries was controlled by DBS programming staff.

The above-described program change control practices increase the risk that unauthorized application programs or program changes may be implemented into the RIMS and AWARE production environments.

**Recommendation: The Department should enhance DVR and DBS program change control practices to provide for the proper authorization, testing, approval, implementation, and documentation of all RIMS and AWARE program changes. As a part of this effort, the Department should review existing written program change control procedures for RIMS and AWARE and, where appropriate, update the procedures to reflect management's current expectations for the performance of these functions. Department management should enforce the performance of the written program change control procedures to promote the ongoing integrity of RIMS and AWARE.**

## IT Application Controls

### Finding No. 15: RIMS Case Management Data

Title 34, Section 361.49, Code of Federal Regulations, provides that, if a designated State unit provides for vocational rehabilitation services for groups of individuals, it must (1) develop and maintain written policies and procedures covering the nature and scope of each of the services it provides and the criteria under which it is provided; and (2) maintain information to ensure the proper and efficient administration of those services in the form and detail and at the time required by the Secretary of the United States Department of Education, including the types of services provided, the costs of those services, and estimates of the numbers of individuals benefiting from those services.

DVR utilized RIMS as the case management system to manage vocational rehabilitation services provided to customers. When services were provided to individual customers, the applicable information was entered into RIMS. However, when group services were provided, the services for the customers within the groups were not being entered into RIMS. Instead, the monetary amounts associated with the group services were entered into the Florida Accounting Information Resource Subsystem (FLAIR). As a result, RIMS reports that were used to provide the number of customers served under other services on Schedule II of the Annual Vocational Rehabilitation Program/Cost Report (RSA-2) did not include customers receiving services within a group setting, as also reported in our report No. 2009-144, State of Florida – Compliance and Internal Controls Over Financial Reporting and Federal Awards dated March 2009. By not entering group services customer information into RIMS, the completeness of RIMS case management data and the reliability and usefulness of reports generated from RIMS was diminished.

**Recommendation: DVR management should ensure that all DVR vocational rehabilitation customer services are entered into RIMS.**

## RELATED INFORMATION

Our IT audit disclosed discrepancies in the DVR and DBS 2007 RSA-2 reports that were produced using, in part, data from RIMS and AWARE and submitted to the United States Department of Education. These matters were reported in our report No. 2009-144, State of Florida – Compliance and Internal Controls Over Financial Reporting and Federal Awards dated March 2009.

## OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts IT 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 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources. An additional objective was to evaluate RIMS and AWARE controls relating to the accuracy of the calculations used to complete Form RSA-2.

The scope of our audit focused on evaluating selected IT controls applicable to RIMS and AWARE during the period August 2008 through November 2008 and selected actions through February 2009.

In conducting our audit, we:

- Interviewed Department and Division personnel.
- Obtained an understanding of RIMS and AWARE, including the processing hardware, software, and user environments; purpose and goals; and the basic data flow through the applications.
- Obtained an understanding of RIMS and AWARE application controls, including reconciliation procedures, input, processing, output, and user controls.
- Obtained an understanding of general IT controls related to RIMS and AWARE.
- Observed, documented, tested, and evaluated key processes and procedures related to the appropriateness of reconciliation procedures between RIMS and FLAIR and AWARE and FLAIR; the appropriateness of selected input, processing, and output control procedures, including the accuracy of the data included in the Form RSA-2; and the adequacy of RIMS and AWARE controls to prevent or detect unauthorized payments to service providers through the use of appropriate access roles.
- Observed, documented, tested, and evaluated key processes and procedures related to the appropriateness of user application access capabilities, including proper separation of duties for RIMS and AWARE.

- Observed, documented, tested, and evaluated key processes and procedures related to physical and environmental safeguards protecting RIMS and AWARE, including the Department's disaster recovery planning.
- Observed, documented, tested, and evaluated key processes and procedures related to the Department's change control process for making modifications to RIMS and AWARE.
- Observed, documented, tested, and evaluated key processes and procedures related to the Department's security program, including procedures for security administration, adequacy of review and removal of access privileges, adequacy of review of access to RIMS and AWARE, and the adequacy of password controls related to RIMS and AWARE.

## AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

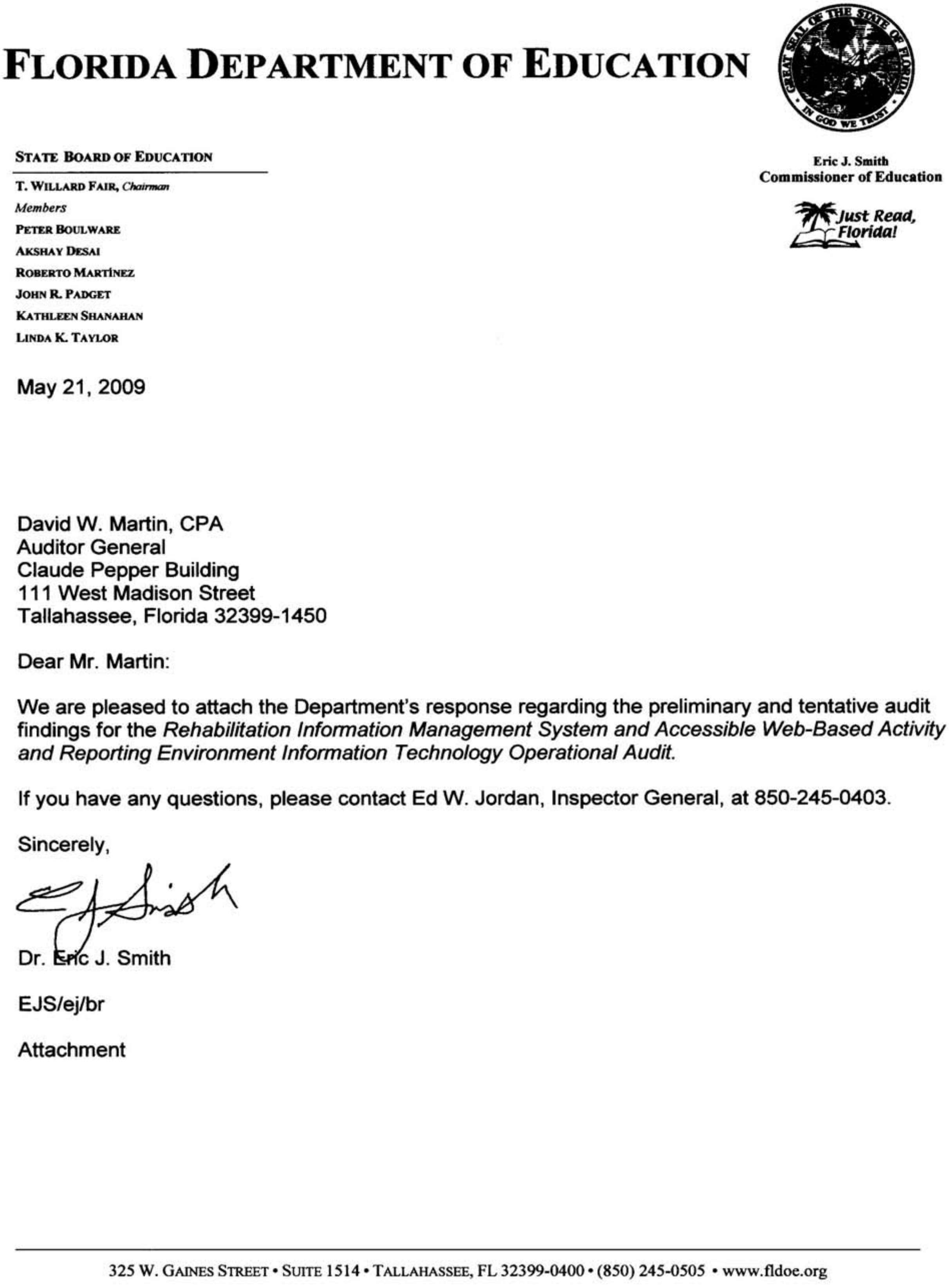
David W. Martin, CPA
Auditor General

## MANAGEMENT'S RESPONSE

In a letter dated May 21, 2009, the Commissioner of Education provided responses to our preliminary and tentative findings. This letter is included at the end of this report as Exhibit A.

THIS PAGE INTENTIONALLY LEFT BLANK

## EXHIBIT A
## MANAGEMENT'S RESPONSE



# FLORIDA DEPARTMENT OF EDUCATION

Eric J. Smith
Commissioner of Education

*Just Read, Florida!*

May 21, 2009

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

Dear Mr. Martin:

We are pleased to attach the Department's response regarding the preliminary and tentative audit findings for the *Rehabilitation Information Management System and Accessible Web-Based Activity and Reporting Environment Information Technology Operational Audit.*

If you have any questions, please contact Ed W. Jordan, Inspector General, at 850-245-0403.

Sincerely,

Dr. Eric J. Smith

EJS/ej/br

Attachment

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

## Preliminary and Tentative Audit Findings
## Rehabilitation Information Management System (RIMS)
## And
## Accessible Web-Based Activity and Reporting Environment (AWARE)
## Information Technology Operational Audit
## May 21, 2009

### Finding 1

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. The OTIS now 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.

### Finding 2

The Department has now 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.

### Finding 3

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.

## EXHIBIT A (CONTINUED)
## MANAGEMENT'S RESPONSE

**Finding 4**
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.

**Finding 5**
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.

**Finding 6**
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.

**Finding 7**
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 II background screening.

**Finding 8**
The Department is currently working to ensure that written security administration procedures are complete and up-to-date and that they adequately address both DBS and DVR systems.

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.

**Finding 9**
The Department is contracting with a vendor to assist with development of DBS security administration procedures in conjunction with developing a process for periodic review of access privileges. To the extent possible given the limitations of a small staff of contract positions, appropriate separation of duties will be addressed. When the ideal separation of application cannot be achieved, the Department will periodically assess the risk and determine if changes are needed.

Additionally, the Department will develop or revise security profiles for MIS staff that prevent update access to specified applications and ensure that security profiles appropriately restrict access to confidential Social Security Information.

**Finding 10**
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.

## EXHIBIT A (CONTINUED)
## MANAGEMENT'S RESPONSE

**Finding 11**
The Department has noted this finding and will continue to address continued improvements in security controls.

**Finding 12**
The Department is no longer using employee social security numbers in RIMS.

**Finding 13**
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.

**Finding 14**
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.

**Finding 15**
The Department is taking steps to ensure that all DVR customer services are entered into RIMS.