FLORIDA DEPARTMENT *of* STATE

CHARLIE CRIST
Governor

KURT S. BROWNING
Secretary of State

December 5, 2008

Kurt S. Browning, Secretary of State
Florida Department of State
R.A. Gray Building
500 South Bronough Street
Tallahassee, FL 32399-0250

Re: Follow-Up Review Applicable to Auditor General Report #2008-187, Department of State Florida Voter Registration System (FVRS) Follow-Up on Prior Audit Findings.

Dear Secretary Browning:

Pursuant to Section 20.055(5)(h), Florida Statutes, the Office of Inspector General (OIG) conducted a follow-up review applicable to the Auditor General's Report as referenced above. We have attached a copy of our report for your review.

As required by law, we have published our report on the status of the corrective actions taken by the Department and filed a copy of such response with the Legislative Auditing Committee.

If you require additional information on this matter please contact me.

Sincerely,

Kirby J. Mole, CIA, CIG, CMA
Inspector General

Att.

cc. Mr. Terry L. Shoffstall, Director, Legislative Auditing Committee
Dawn K. Roberts, Assistant Secretary of State/Chief of Staff
John Boynton, Director, Division of Administrative Services
Don Roberts, Chief Information Officer

R. A. Gray Building • 500 South Bronough Street • Tallahassee, Florida 32399-0250
Telephone: (850) 245-6500 • Facsimile: (850) 245-6125
www.dos.state.fl.us

JLAC
Rec'd 12/9/08

FLORIDA DEPARTMENT OF STATE-OFFICE OF INSPECTOR GENERAL STATUS REPORT FOR CORRECTIVE ACTION FOR AUDITOR GENERAL'S REPORT NO. 2008-187 DEPARTMENT OF STATE FLORIDA VOTER REGISTRATION SYSTEM (FVRS) FOLLOW-UP ON PRIOR AUDIT FINDINGS INFORMATION TECHNOLOGY AUDIT

- - -

December 5, 2008

The purpose of this follow up review is to report on the current status of corrective actions taken by the Department of State (Department) in response to the recommendations made by the Auditor General in Report No. 2008-187. The Auditor General's information technology audit focused on determining the status of corrective actions regarding prior audit findings disclosed in Auditor General Report No. 2006-194, findings Nos. 10 through 12, relating to Department information technology (IT) controls over FVRS. Audit report No. 2008-187 included the period July 2006 through February 2008 and selected Department actions through March 2008.

Auditor General's Finding No. 1: A comprehensive IT risk assessment of FVRS had been performed and the Department was in the process of addressing the risks identified in the risk assessment report. However, the Department's written policies and procedures for authorizing access to FVRS needed enhancement and the Department had not established written policies and procedures for monitoring and terminating access to FVRS.

Auditor General's Recommendation No. 1 and 2:

1. The Department should establish controls to reduce or eliminate the risks identified in its comprehensive risk assessment of FVRS. In addition, the Department should perform a comprehensive risk assessment of FVRS every three years.

2. The Department should enhance the written policies and procedures for authorizing Department and county employee access to FVRS to address all components of the authorization process. Also, the Department should establish written policies and procedures for monitoring and terminating Department and county employee access to FVRS.

Department's Statement of Corrective Action(s) Implemented:

1. A comprehensive risk assessment for FVRS was completed in July of 2006 and it identified seven items for improvement. The Department has or is addressing all seven items in the following manner:

A. The separation of duties has been mitigated by the addition of extra positions within FVRS. The positions were filled in late 2006 and have allowed for additional separation where previously none was available.
B. All 67 counties have executed an MOU with the Department that outline the minimum requirements to access FVRS. This is being augmented with the introduction of the specific procedures for county security administration. These procedures are DOSIT-01-06-A006 FVRS County SSA Guide and DOSIT-01-06-A005 Access Controls for FVRS Users. These procedures are currently in draft form and in the approval process.
C. The Department has recently installed a Network Access Control solution to provide detailed traffic auditing and reporting. This will significantly enhance the FVRS security manager's ability to monitor access to critical system components. The security manager is also in the process of producing additional security administration procedures to enhance the effectiveness of the FVRS security environment. Procedure DOSIT-01-06-A005 Access Controls for FVRS Users is in draft form and in the approval process.
D. The FVRS security manager is in the process of developing a detailed security program that addresses Department and county access controls within FVRS. This program will address the FVRS users and the county system security administrators. The procedure DOSIT-01-06-A005 Access Controls for FVRS Users is in draft form and in the approval process.
E. The FVRS security manager has developed a script to monitor application access and to provide alerts when exceptions are noted. This script is completed and in production at this time. The application programs also audit pertinent data changes submitted to the system for processing. These changes are logged by user-id and date/time and are available for reporting and monitoring as needed.
F. The FVRS security manager is in the process of creating a number of security administration procedures to enhance the access control to FVRS. Specifically these documents are "DOSIT-01-06-A005 Access Controls for FVRS Users", "DOSIT-01-06-A004 Access Controls for FVRS Machine Access", "DOSIT-01-06-A007 FVRS County Contact Maintenance", and "DOSIT-01-06-A006 FVRS County SSA Guide". These procedures are in draft form and in the approval process.
G. The infrastructure deficiencies addressed by the risk assessment in 2006 identified the need for protection against the interruption of power and/or against generated or induced electromagnetic radiation and protection against ambient temperature and humidity fluctuations. The DCF data center to which the DOS data center moved in the fall of 2007 has provided significant improvements in the protection against the interruption of power, against generated or induced electromagnetic radiation, and against ambient temperature and humidity fluctuations. The new facility has also significantly enhanced the physical security controls of the FVRS system.

The Department completed a risk assessment for the FVRS system and delivered the risk assessment to the Office of Information Security on November 13, 2008.

2. The Department has in draft form the following procedures that address county and Department employee authorization. These procedures are currently moving through the approval process:

   A. "DOSIT-01-06-A005 Access Controls for FVRS Users" - Procedure created and in use, ready for final update, review, and approval. This document covers all aspects of access to FVRS as a user, especially Dept of State users. It also provides instructions for State Security Administrators as they assist County System Security Administrators (SSA's). This procedure also defines monitoring and audit requirements, including periodic production of user reports that are sent to County SSA's on a periodic basis.

   B. "DOSIT-01-06-A004 Access Controls for FVRS Machine Access" - Procedure created and in use, however is still in draft form. Procedure addresses access to the machines that support the FVRS functions. This affects about a dozen people who, according to the FVRS System Security Plan are, Systems/Network Administrators, Applications/Database Administrators, or Security Administrators.

   C. "DOSIT-01-06-A006 FVRS County SSA Guide" - This is a greatly expanded version of the original document that was created in 2005. It has been created and submitted to the county SSA's (designated security personnel) for comment. It is now ready for final comment, update, and approval. In addition to describing the specific tasks of adding and removing users from the FVRS system, the document provides guidance on greater security policy issues and references the existing Memorandum of Agreement to continue to establish ground rules for development of an overall Interagency Information Security Program. It also specifies a required response to the periodic user reports that are prepared by the FVRS Info Sec Admin.

Status of Corrective Actions:

The Department completed the corrective actions shown above as 1A, 1E, and 1G. The Department is working to implement corrective actions 1B, 1C, 1D, 1F and 2A through 2C. The Department estimates that it will complete the corrective actions on or before January 31, 2009.

Auditor General's Finding No. 2: Although some policies and procedures had been developed, the Department's IT governance model continued to lack important provisions relating to the management, use, and operation of FVRS.

Auditor General's Recommendation No. A, B, C, D & E:

A. The Department, in conjunction with the county Supervisors of Elections' offices, should develop a formal security program for FVRS that includes written directives, including policies and procedures, or governance addressing the minimum security measures needed to support and protect the FVRS business purpose and the confidentiality, availability, and integrity of data contained therein.

B. Specifically, written policies and procedures should be established to address access authorization and review, logical access controls, and user awareness training, including a county System Security Administrator security awareness training program.

C. The Department should update the IT disaster recovery plan to include FVRS as well as other noted deficiencies addressed by the Gap Analysis.

D. The Department should implement a formal process for monitoring and reviewing the audit logs to identify specific unauthorized access attempts to penetrate the system and to identify any unauthorized procedures performed by authorized users.

E. The Department should implement appropriate written policies and procedures to designate employee positions within the Division of Elections or otherwise connected with FVRS that, because of special responsibility or sensitive job duties, require background checks and fingerprinting. Furthermore, the Department should ensure that employees already occupying those positions have been subjected to level two background checks including fingerprinting.

Department's Statement of Corrective Action(s) Implemented:

A. The Department has completed a draft of the county SSA guide that is currently under review by the counties. This document provides the guidelines for FVRS security administration in the counties. This document is described as:

- "DOSIT-01-06-A006 FVRS County SSA Guide" - this is a greatly expanded version of the original document that was created in 2005. It has been created and submitted to the county SSA's (designated security personnel) for comment. It is now ready for final comment, update, and approval. In addition to describing the specific tasks of adding and removing users from the FVRS system, the document provides guidance on greater security policy issues and references the existing Memorandum of Agreement to continue to establish ground rules for development of an overall Interagency Information Security Program. It also specifies a required response to the periodic user reports that are prepared by the FVRS Info Sec Admin.

B. The Department is in the process of developing a security and awareness training program. This program includes:

- A Security Awareness presentation is nearly complete and is intended for presentation to all users – including BVRS employees, and Supervisors of Elections and their staff.
- A Security Training presentation has been outlined and is intended for presentation to specific units, such as BVRS.
- A Security Education presentation has been outlined and is intended for technical and security staff – particularly County SSA's.

- "DOSIT-01-06-A007 FVRS County Contact Maintenance.doc" – Procedure defines the maintenance required for critical contact information of Supervisors of Elections, Security Contacts, Technical Contacts, and Vendors. This ongoing contact is essential to building the relationships upon which a program can be founded.
- Notices of particular interest are regularly forwarded to a special interactive distribution list that includes all designated County Security Administrators. These notices are items such as:
    - Vulnerability alerts from organizations such as US-CERT or the Multi-State Information Sharing and Analysis Center (MS-ISAC).
    - Relevant discussion topics that appear in Info Sec Blogs. Unusual events are examined further.

C. The Department is in the process of creating a disaster recovery plan that includes FVRS.

D. The Department has implemented a process to monitor and review the access audit logs to identify specific unauthorized access attempts to penetrate the system and to identify any unauthorized procedures performed by authorized users. A script is now in production that produces a daily report of failed access attempts to the FVRS transaction system. All members of the FVRS security team receive email alerts with regard to this matter.

E. The Department has completed the transition of all 52 employees associated with FVRS to positions of special trust. These positions have all had the FBI Level II check completed.

Status of Corrective Actions:

The Department is in the process of implementing corrective actions for 2A through 2C. The Department has completed the corrective actions for 2D and 2E.

Auditor General's Finding No. 3: Although the Department had put measures in place to help ensure the integrity of data in FVRS, improvements were still needed in the comprehensive check of all felony convictions against all voters.

Auditor General's Recommendation No. 8

8. The Department should evaluate the risk to the State of not performing the match. If a significant risk exists, such as a negative impact on the State's voting process, the Department should explore various methods of acquiring the resources and select a solution that would allow staff to perform the systematic felon match against all existing voter registrations.

Department's Statement of Corrective Action(s) Implemented:

The Department continues to evaluate systematic felon matching and is working with different agencies involved with the reporting of criminal felony history to enhance data exchanges. The completion of the new workflows will be critical to an analysis of a comprehensive match process. It is important to note that the Department has measures in place to systematically match all new and existing registrations that are updated or otherwise changed against felony conviction files. Furthermore, the entire voter registration list is matched against all new felony or changed felony records reducing the number of registrants who have not been matched. These two processes and the gradual attrition of voters due to movement or deceased status will continue to reduce the number of registrants who may not have been initially matched against the felon file.

Status of Corrective Actions:

Even though the Department has not prepared a formal document to report its current evaluation of the felon matching process, the Department continues to explore data sources and expend Department's resources for processes, such as shown above, to expand the felon matching process to all existing registered voters.