AUDITOR GENERAL

DAVID W. MARTIN, CPA

DEPARTMENT OF STATE
FLORIDA VOTER REGISTRATION SYSTEM (FVRS)
FOLLOW-UP ON PRIOR AUDIT FINDINGS

Information Technology Audit

SUMMARY

Section 303 of the Federal Help America Vote Act of 2002 (HAVA), Public Law 107-252, requires states to implement a centralized voter registration system. Florida's Statewide voter registration system is the Florida Voter Registration System (FVRS) and is maintained by the Department of State (Department).

Our audit focused on determining the status of corrective actions regarding prior audit findings disclosed in audit report No. 2006-194, finding Nos. 10 through 12, relating to Department information technology (IT) controls over FVRS. Our audit, which included the period July 2006 through February 2008 and selected Department actions taken through March 2008, concentrated on Department actions and did not include a review of procedures at the 67 county Supervisors of Elections' offices.

The results of our follow-up audit are summarized below:

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.

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.

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.

BACKGROUND

HAVA sets forth the requirement that each state, acting through the chief state election official, shall implement, in a uniform and nondiscriminatory manner, a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the state level. In accordance with HAVA legislation, the centralized statewide voter registration system shall store, manage, and retrieve the official list of registered voters throughout the state; contain the name and registration information of every legally registered voter in the state; assign a unique identifier to each legally registered voter in the state; and coordinate with other agency databases within the state.

In accordance with Section 98.035, Florida Statutes, the Department is responsible for implementing, operating, and maintaining FVRS. Further, the Department may adopt rules governing the access, use, and operation of FVRS to ensure security,

uniformity, and integrity of the system. Provisions are included in the law to allow the county Supervisors of Elections' offices to use hardware or software they choose, provided that such hardware or software does not conflict with the Department's operation of FVRS. As discussed in the Department's Guide to FVRS, the Department has assumed responsibility for certain verifications that data transactions are valid and are received only from authorized sources to protect the integrity of the FVRS data.

On January 1, 2006, FVRS became fully operational Statewide pursuant to HAVA requirements. Pivotal to the design of FVRS was the retention of county voter registration systems. Each of the 67 counties was to remediate its voter registration system to accommodate an FVRS interface and operating specifications. In response to the new HAVA responsibilities, the Department established a Bureau of Voter Registration Services (Bureau) within the Division of Elections. The Bureau oversees the voter registration requirements of HAVA and Florida law. Each county is to retain the greatest level of autonomy over county voter registration systems while interfacing with FVRS to exchange information.

In accordance with Section 98.015, Florida Statutes, each county Supervisor of Elections is responsible for updating voter registration information, entering new voter registrations into the Statewide voter registration system, and acting as the official custodian of documents received by the Supervisor related to the registration and changes in voter registration status of electors of the Supervisor's county. While the Department is responsible for the overall security and integrity of FVRS, each county Supervisor of Elections is responsible for ensuring that all voter registration and voter list maintenance procedures conducted are in compliance with any applicable requirements prescribed by rules of the Department through the Statewide voter registration system or prescribed by the Voting Rights Act of 1965, the National Voter Registration Act of 1993, or HAVA.

FINDINGS AND RECOMMENDATIONS

Our prior audit disclosed 11 Department IT control issues relating to FVRS where improvement in the areas of IT risk management, IT governance, and FVRS data integrity was needed. This follow-up audit disclosed that the Department had made progress in improving some FVRS controls in the identified areas, but other findings remained unresolved. Specifically, of the 11 FVRS control issues disclosed in the prior audit, the Department had corrected 3, partially corrected 6, and had not corrected 2. Details of the status of the Department's corrective actions relating to the prior audit findings, as of March 2008, are disclosed in Table 1 below.

Definitions of Prior Audit Finding Status

- **Corrected:** Successful development and use of a process, system, policy, or control to correct a prior audit finding.
- **Partially Corrected:** A process, system, policy, or control to correct a prior audit finding was not completely developed or was successfully developed but was not consistently or completely used.
- **Not Corrected:** Preliminary analyses have been performed for correcting the prior audit finding, but the finding has not yet been corrected.

Table 1: STATUS OF PRIOR AUDIT FINDINGS NOTED IN AUDIT REPORT NO. 2006-194 AS OF MARCH 2008

Finding No.	Bullet No.	Prior Audit Report Finding Issue	Condition Noted in Current Audit	Current Recommendation
			Finding No. 1: IT Risk Management	
10	1	The Department had not completed a formal risk assessment of FVRS.	**Partially Corrected:** The Department contracted with Integrated Computer Solutions, Inc. (ICS), to perform a comprehensive IT risk assessment of FVRS. The risk assessment was completed and a final report issued on July 5, 2006. The ICS report concluded that seven items identified required improvements. The Department developed an action plan addressing the seven items. Regarding the seven items, on March 17, 2008, the Department indicated that one item relating to separation of duties had been corrected. Physical security control issues reported by ICS were to be corrected with the move of the data center to a new location. We did not evaluate physical security controls since physical security issues were outside the scope of our follow-up audit. The remaining five items from the risk assessment had not been completely corrected. In addition, the Department had not readdressed the infrastructure portion of the comprehensive risk assessment of FVRS following the move of the data center to the new location in September 2007. Pursuant to Section 282.318(2)(a)2., Florida Statutes, comprehensive risk assessments are to be updated every three years. The Department's comprehensive risk assessment of FVRS will be three years old in July 2009. In response to audit inquiry, Department staff indicated that the relocation of the data center and offices had limited the availability of staff resources to perform another risk assessment. Department staff further indicated that they plan to perform another comprehensive risk assessment of FVRS by September 2008.	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.
10	2	Authorizations for access to Department resources had not been properly documented for all FVRS users and access capabilities were not timely revoked or modified as necessary for individuals who had terminated employment. In addition, the Department did not have a formal process in place for the periodic monitoring of actual access capabilities through comparison to the authorizations.	**Partially Corrected:** Policies and procedures for authorizing Department and county employee access to FVRS were not complete. During the audit period, no policies or procedures had been established for determining the level of FVRS access to be granted related to job duties. We also noted that authorizations for access to Department resources were not completely documented for all FVRS users. In response to audit inquiry, Department staff stated that they had recently implemented a policy regarding the FVRS access levels of employees. The County Security System Administrator Guide outlines the process for issuing access but does not include detailed procedures for issuing access. An intraweb application was informally recommended by the Department as the system to be used by the Department and the counties for submitting access change requests, but no policies and procedures existed to require a specific method.	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.

Finding No.	Bullet No.	Prior Audit Report Finding Issue	Condition Noted in Current Audit	Current Recommendation
			Policies and procedures for monitoring and terminating Department and county employee access did not exist. Access monitoring had not taken place on a consistent basis and there was no formally established frequency for monitoring Department or county user accounts. Access capabilities were not timely removed or modified as necessary for some individuals who had terminated their employment or changed job duties. In our testing of all 49 Bureau user accounts having access privileges granted to FVRS, we noted that two former employees who terminated employment on December 14, 2007, and March 6, 2008, still had access privileges to FVRS. The Department removed these access privileges on March 25, 2008, and March 26, 2008, respectively. Additionally, three employees had been granted FVRS access privileges on October 17, 2007, to temporarily assist with voter registration applications. Upon audit inquiry, Department staff stated that the three employees no longer needed the access privileges and removed access for one of the three on March 25, 2008, and removed access for the other two on March 27, 2008.	
			Finding No. 2: IT Governance Model	
11	1	The Department, in conjunction with the county Supervisors of Elections' offices, had not developed a formal security program for FVRS. The Department had not developed formal written directives or guidance to ensure a consistent approach and enforcement across all environments in such matters as configuration management, virus protection, system software maintenance and updates, and patch management.	**Partially Corrected:** The ICS risk assessment report issued on July 5, 2006, as discussed above, noted that the Department was lacking an agencywide information security program to review and evaluate the information security policies, procedures, and standards for FVRS, including the county Supervisors of Elections' offices. The risk assessment also found that Memoranda of Understanding or service-level agreements with the county Supervisors of Elections' offices were needed to address the minimum security access requirements for FVRS. The Department had rulemaking authority but had chosen to use policies and procedures to provide guidance to the county Supervisors of Elections' offices relating to the security of FVRS. Various security-related policies and procedures had been developed and implemented by the Department. Also, by December 2006, the Department had executed Memoranda of Understanding with the 67 county Supervisors of Elections' offices regarding provisions for emergency election support. However, three procedures documents (Guide to FVRS, FVRS Security Approach Plan, and County Security System Administrator Guide) had not been updated since our prior audit. These documents addressed the roles and responsibilities of the Department, county Supervisors of Elections' offices, and the county Security System Administrators.	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.

Finding No.	Bullet No.	Prior Audit Report Finding Issue	Condition Noted in Current Audit	Current Recommendation
			The Department had created a FVRS System Security Plan that reported the status of the items being addressed but did not indicate cost-effective controls that would be used to reduce or eliminate identified risks, including risks applicable to the county Supervisors of Elections' offices. In response to audit inquiry, Department staff indicated that they did not plan to continue to maintain the Guide to FVRS and the FVRS Security Approach Plan. The roles and responsibilities of the Department, county Supervisors of Elections' offices, and county Security System Administrators addressed in these documents were not included in the latest version of the FVRS Security System Plan and may not be updated as indicated by the Department's response to audit inquiry. Other than the items listed above relating to the policies and procedures, the Department, as of March 2008, had not addressed directives or guidance to ensure a consistent approach and enforcement across all environments for such matters as configuration management, virus protection, systems maintenance and updates, and patch management.	
11	2	Guidelines to promote consistent, effective policies and procedures related to information resource classification and control, access authorization and review, distribution of user roles, logical access controls, and user security awareness training had not been developed by the Department. Additionally, while the Guide to FVRS stated that training in user/identity management will be required of State and county System Security Administrators, the Department had not yet conducted a formal training program.	**Partially Corrected:** The information resource classification and control and distribution of user roles were addressed in the FVRS System Security Plan. The FVRS System Security Plan did not address guidelines to promote consistent, effective policies and procedures related to access authorization and review, logical access controls, and user security awareness training. Additionally, the ICS risk assessment disclosed that there was inadequate security awareness and training and, at a minimum, the training should take place annually and be documented. The Department did not have a county Security System Administrator security awareness training program; however, the System Programming Administrator had begun a gap analysis to identify issues to be addressed in the county Security System Administrator training program.	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.
11	3	The Department was in the process of, but had not completed, the integration of FVRS system planning into its overall IT disaster recovery plan. In addition, although the Department indicated that disaster recovery plans had been requested from each county, there was no formal, written process in place for receiving and evaluating those plans to ensure their adequacy in recovering timely from a disruption to operations.	**Not Corrected:** The Department still had not incorporated FVRS into the IT disaster recovery plan. The Department had an IT Disaster Recovery Plan Gap Analysis that identified other deficiencies in the Department's IT disaster recovery plan in addition to not including FVRS. However, the recommendations outlined in the IT Disaster Recovery Plan Gap Analysis had not been implemented.	The Department should update the IT disaster recovery plan to include FVRS as well as other noted deficiencies addressed by the Gap Analysis.

Finding No.	Bullet No.	Prior Audit Report Finding Issue	Condition Noted in Current Audit	Current Recommendation
11	4	The Department had not devised a formal process for review and retention of the logs of unauthorized attempts to penetrate the system and unauthorized procedures by authorized users.	**Partially Corrected:** The Department still lacked a formal process for review and retention of the security violation and activity logs for FVRS. Although FVRS generated audit logs of various activities of the system, such as security violation and activity logs and the logs had a longer retention period than before, the Department had not yet implemented a process for monitoring and reviewing the audit logs, and exception reports were not generated to identify the specific unauthorized access attempts.	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.
11	5	The Department had not designated any individual positions in connection with FVRS or the Division of Elections as positions of special trust. Therefore, level two (Federal Bureau of Investigation) screenings had not been performed.	**Not Corrected:** The Department had still not designated any individual positions in connection with FVRS or the Division of Elections, including Bureau employees, as positions of special trust. The Department required all new and existing employees to submit a Standard of Conduct Form to ensure that they acknowledge the confidentiality of information within FVRS and affirm that they will only utilize the system within the defined parameters. Additionally, all new hires are required to submit to level one (Florida Department of Law Enforcement) background screening; however, there were no documented policies and procedures relating to this requirement and neither level two screening nor fingerprinting was performed.	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.
			Finding No. 3: FVRS Data Integrity Procedures	
12	1	The Department had not yet implemented a systematic process to periodically scan for and identify duplicate registrations in FVRS.	**Corrected:** On May 9, 2006, the Department implemented a monthly process to systematically identify potential duplicate records and distribute this information via compact disks to the 67 counties. According to Department staff, the FVRS Program Manager is working with vendors to create an appropriate interface that will allow the information to be transmitted to the counties electronically.	N/A
12	2	Although the Department had a systematic process in place for identifying potential felon matches within FVRS, it had not completed a comprehensive check of all felony convictions against all voters.	**Partially Corrected:** The Department still had not completed a comprehensive check of all felony convictions against all voters. There were approximately 10.5 million voters on the voter registration list prior to the implementation of FVRS. Department staff stated that running the match on the prior registrants would not be a problem, but a lack of resources would prevent staff from working the output produced by the match. Staff further stated that they were busy full-time working the output from the most recent registration felon match process and, by the time they could process the backlog, the data would be stale and not useful.	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.
12	3	The Department indicated that there had been instances where data supplied by external agencies was not accurate or timely. For example, records that were supplied by the Office of Vital Statistics for the purpose of matching for deceased voters had, at times, contained inaccurate social security numbers. Additionally, the Department indicated that data received from the Office of Vital	**Corrected:** According to Department staff, the Office of Vital Statistics performed some database work that improved the accuracy and reduced the time delays of the data transmitted to the Department related to deceased individuals. Our review of Department records, for example, disclosed that the Department, in January 2008, received 5,610 Office of Vital Statistics matches within 30 days after the date of death, whereas in June 2006, there were no matches within 30 days. In June 2006, it took 106 days to obtain approximately the same number of matches, which was approximately 3.5 times longer.	N/A

Finding No.	Bullet No.	Prior Audit Report Finding Issue	Condition Noted in Current Audit	Current Recommendation
		Statistics, though received regularly, may lag as much as two to three months.		
12	4	The Department had not formalized a process by which to determine whether Supervisors of Elections have satisfactorily met the statutory requirement of certifying to the Department no later than July 31 and January 31 of each year, activities conducted, during the first and second six months of the year respectively, regarding procedures for removal of voters determined to be ineligible.	**Corrected:** The Department had formalized the statutorily required certification process for the county Supervisors of Elections. The Department had also created forms for the Supervisors of Elections to use to certify List Maintenance Activities and Voter Registration Activities. These activities helped to ensure that ineligible voters are removed from FVRS. The Bureau created a check-off list of all counties for each certification. As certifications from the counties were received, Bureau staff checked each county off the list. As the deadline approached, Bureau staff began calling the counties that had not submitted their certifications to ensure that all certifications were received by the deadline. According to Department staff, all 67 counties were in compliance and had submitted certifications to the Department for all four of the certification periods that have occurred since implementing FVRS.	N/A

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the extent to which the Department corrected, or was in the process of correcting, deficiencies disclosed in audit report No. 2006-194 that are applicable to FVRS.

The scope of our audit focused on evaluating the Department's corrective actions regarding IT control deficiencies applicable to the FVRS disclosed in finding Nos. 10 through 12 of the prior audit during the period July 2006 through February 2008, and selected actions taken through March 2008. A determination of the status of Department corrective actions regarding finding Nos. 1 through 9 of audit report No. 2006-194 was not within the scope of this IT audit but was performed in our Federal Awards and operational audits of the Department (see audit report Nos. 2008-141 and 2007-146). Our follow-up audit also did not include a review of procedures at the 67 county Supervisors of Elections' offices. Furthermore, physical security controls at the Department were not within the scope of this follow-up audit. In conducting our audit, we interviewed appropriate Department personnel, observed Department processes and procedures, and performed various other audit procedures to test selected IT controls related to FVRS.

We conducted this IT audit in accordance with applicable 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.

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 audit.

David W. Martin, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated June 6, 2008, the Secretary of State provided responses to our preliminary and tentative findings. This letter is included at the end of this report as APPENDIX A.

This audit was conducted by Shera Bake, CISA, and supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, via 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 (http://www.myflorida.com/audgen/); by telephone (850) 487-9024; or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

THIS PAGE LEFT BLANK INTENTIONALLY

APPENDIX A

MANAGEMENT RESPONSE

FLORIDA DEPARTMENT of STATE

CHARLIE CRIST
Governor

KURT S. BROWNING
Secretary of State

June 6, 2008

David W. Martin
G74 Claude Pepper Building
Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Re: The Information Technology Audit of the Department of State, Florida Voter Registration System, Follow-up on Prior Audit Findings

Dear Mr. Martin:

Please accept this letter as the Department's response to your e-mail dated May 8, 2008, applicable to the audit referenced above.

Please do not hesitate to contact me if you have any further question.

Dawn K. Roberts
Assistant Secretary/Chief of Staff

aw

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

FLORIDA DEPARTMENT OF STATE
Response to the Auditor General's
Preliminary and Tentative Audit Findings and Recommendations

Florida Voter Registration System (FVRS)
Follow-Up On Prior Audit Findings
Information Technology Audit
For the Period July 2006 through February 2008 and Selected Actions taken through March 2008

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.

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 Response to Recommendation No. 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

1. 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.
2. 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.
3. 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
4. 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.
5. The FVRS security manager has developed a script to monitor application access and to provide alerts when exceptions are noted. This script is currently in testing and is expected to be in production before the end of the year. 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.

6. 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 will be completed before the end of the current year.
7. 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 its last comprehensive risk assessment in July of 2006, and plans to have another assessment completed in July of 2009.

Department's Response to Recommendation No. 2:

The FVRS security manager is in the process of addressing the deficiencies in the procedures for authorizing Department and county employees' access to FVRS and for monitoring and terminating employee access. Specifically, the FVRS security manager has submitted for approval the procedure "DOSIT-01-06-A005 Access Controls for FVRS Users" which addresses the Department employees' access to FVRS. The security manager is currently writing the procedure "DOSIT-01-06-A006 FVRS County SSA Guide" which addresses the county employees' access to FVRS.

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.

Recommendation No. 3, 4, 5, 6 & 7:

3. 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.

4. 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.

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

6. 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.

7. 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 Response to Recommendation No. 3:

The FVRS security manager plans to establish a security awareness training and outreach program for the Department's FVRS employees and the county system security administrators. The program will address the minimum security measures required to support the FVRS business purpose and the confidentiality, availability, and integrity of the data.

Department's Response to Recommendation No. 4:

The FVRS security manager is currently working to fully define, formalize, and publish procedures that address access authorization and review, logical access control, and security training issues. 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".

Department's Response to Recommendation No. 5:

The FVRS administration will have a FVRS disaster recovery plan developed in FY 2008/2009.

Department's Response to Recommendation No. 6:

The FVRS security manager has developed a script to monitor application access and to provide alerts when exceptions are noted. This script is currently in testing and is expected to be in production in September 2008.

Department's Response to Recommendation No. 7:

The Division of Elections will implement written policies and procedures to designate FVRS employee positions as positions of special trust with required background checks and fingerprinting.

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.

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 Response to Recommendation No. 8:

The Division of Elections will evaluate the risk to the State of not performing a comprehensive check of all felony convictions against all voters in our database, and explore the resources and staff necessary to perform a systematic felon match against all existing voter registrations.

THIS PAGE LEFT BLANK INTENTIONALLY