STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2016-002
July 2015

DEPARTMENT OF STATE

Florida Voter Registration System (FVRS)

Sherrill F. Norman, CPA
Auditor General

Secretary of State

Section 20.10, Florida Statutes, creates the Department of State. The head of the Department is the Secretary of State who is appointed by the Governor and subject to confirmation by the Senate. Ken Detzner served as Secretary of State during the period of our audit.

The team leader was Suzanne Varick, CPA, and the audit was supervised by Tina Greene, CPA, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General are available at:

www.myflorida.com/audgen

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

DEPARTMENT OF STATE

Florida Voter Registration System (FVRS)

SUMMARY

Section 303 of the Federal Help America Vote Act of 2002 (HAVA), Public Law 107-252, requires each state to implement a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the state level. The computerized list shall serve as the single system for storing and managing the official list of registered voters throughout the state. Florida's Statewide voter registration list, implemented on January 1, 2006, is the Florida Voter Registration System (FVRS), a database maintained by the Department of State (Department).

This operational audit focused on evaluating selected information technology (IT) controls applicable to the FVRS and included a follow-up on the findings included in our report No. 2008-187 that were applicable to the scope of this audit. As summarized below, the audit disclosed areas in which improvements in FVRS IT controls were needed.

Finding 1: Department FVRS IT maintenance controls needed improvement.

Finding 2: Department FVRS performance and capacity monitoring controls needed improvement.

Finding 3: Although the Department had a Disaster Recovery Plan (Plan) in place for the FVRS, the Plan had not been tested since April 2011.

Finding 4: Some inappropriate and unnecessary access privileges existed in the Voter Focus application that is used to enter data into the FVRS.

Finding 5: The Department had not established a mechanism to provide reasonable assurance that all changes implemented into the FVRS production database environment were properly authorized, tested, and approved.

Finding 6: Security awareness training for members of the Department workforce hired since July 1, 2014, had not been conducted in a timely manner.

Finding 7: Certain Department security controls related to protection of confidential and exempt data, software support, authentication, logging, and separation of duties needed improvement.

BACKGROUND

As head of the Department, the Secretary of State acts as the Chief Election Officer and is responsible for the creation and administration of the Statewide voter registration list as required by the Federal Help America Vote Act of 2002 (HAVA). The Secretary of State also facilitates voter registration, voting, and the conduct of elections in coordination with the 67 county Supervisors of Elections.

Pursuant to Section 98.015(3), 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 of electors and changes in voter registration status of electors of the

Supervisor's county. The Statewide voter registration system is a database known as the Florida Voter Registration System (FVRS). The Bureau of Voter Registration Services staff within the Department use the Voter Focus application to enter voter registration data in the FVRS. Section 98.035(5), Florida Statutes, provides that the Department may adopt rules governing the access, use, and operation of the FVRS to ensure security, uniformity, and integrity of the system.

FINDINGS AND RECOMMENDATIONS

Finding 1: FVRS IT Maintenance Controls

IT maintenance controls ensure that routine maintenance is scheduled, performed, and documented to reduce the risk of equipment failures and help identify problem areas that may require corrective action. Effective IT maintenance controls include the following:

- Maintenance schedules that prescribe the frequency and type of preventative maintenance to be performed including maintenance in accordance with IT-vendor specifications.
- Maintenance records of maintenance performed, problems and delays that are encountered, the reasons for the problems and delays, and the elapsed time for the resolution of the problems and delays.
- Routine analyses of maintenance records to identify any recurring patterns or trends that may require additional review and evaluation.

In conducting this audit, we determined that the Department was unable to provide appropriate documentation to evidence that effective FVRS IT maintenance controls were in place and functioning. Specifically, we noted that the Department did not have maintenance schedules that prescribed the frequency and type of preventative maintenance to be performed. Additionally, the Department did not have records of scheduled and unscheduled maintenance that included complete information on all maintenance performed, problems and delays that were encountered during the maintenance process, the reasons for the problems and delays, the elapsed time for the resolution of the problems and delays, and routine analysis of maintenance records to identify recurring patterns or trends that may have required additional review and evaluation by management. Furthermore, on March 4, 2015, subsequent to our audit inquiry, Department staff provided a manually prepared spreadsheet of FVRS unscheduled downtimes (i.e., system unavailability) on which the Department listed eight unscheduled downtimes between December 2014 and February 2015. Our review of the manually prepared spreadsheet disclosed that for the identified unscheduled downtimes in February 2015 the FVRS was unavailable for various time intervals on February 10, 11, and 12 and for a continuous duration from February 24 through 26.

Without appropriate documentation to evidence that effective FVRS IT maintenance controls are in place, management may not be able to ensure that IT failures, should they continue to occur, will be detected and resolved in a timely manner.

Recommendation: The Department should improve FVRS IT maintenance controls to include appropriate documentation of maintenance schedules, maintenance records, and routine analyses of maintenance records.

Finding 2: FVRS Performance and Capacity Monitoring Controls

Section 303 of HAVA requires each State to implement a single, uniform, official, centralized, interactive computerized Statewide voter registration list and that any election official in the State may obtain immediate electronic access to the information contained in the computerized list. Effective performance and capacity monitoring controls balance current and future needs for availability, performance, and capacity to meet end-user needs.

Our review disclosed that FVRS performance and capacity monitoring controls needed improvement. Specifically, the Department was unable to provide documentation of the following to evidence appropriate FVRS performance and capacity monitoring:

- Written performance and capacity monitoring procedures.
- Written procedures or protocols for County users to report performance issues to Department IT management.
- Service-level agreements between the Department and the Counties documenting acceptable performance levels.
- An initial assessment and performance baseline of database statistics that should be used for current and future comparisons of database performance and capacity.
- Reports of database metrics, alerts, and notification processes.
- Routine review of the aforementioned performance and capacity documents to ensure appropriate ongoing availability, performance, and capacity to meet end-user needs.

The lack of appropriate FVRS performance and capacity monitoring controls increases the risk that significant availability, performance, or capacity issues, should they continue to occur as noted in Finding 1, may not be timely identified and resolved.

Recommendation: The Department should improve FVRS performance and capacity monitoring controls.

Finding 3: Disaster Recovery Plan Testing

Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-1.012(4), Florida Administrative Code, provides that information technology resources identified as critical to the continuity of governmental operations shall have documented disaster recovery plans to provide for the continuation of critical agency functions in the event of a disaster. AEIT Rule 71A-1.012(5), Florida Administrative Code, and the Department's *Contingency Planning Policy (DOSIT-01-20-14)* state that IT disaster recovery plans shall be tested at least annually. Effective testing of disaster recovery plans provides an important measurement of the feasibility of the plans in ensuring the continuity of critical agency functions. Additionally, testing helps determine how well Department resources have been prepared to function effectively in a disaster situation.

[1] Chapter 2014-221, Laws of Florida, effective July 1, 2014, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; pending issues and existing contracts; administrative authority; administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, in effect as of November 15, 2010; trust funds; and unexpended balances of appropriations, allocations, and other funds of the AEIT to the AST.

According to Department management, although the Department had a Disaster Recovery Plan (Plan) in place for the FVRS, the Plan had not been tested since April 2011. Without timely testing of the Plan, the risk is increased that the Plan and resources will not effectively function as intended in an emergency situation to ensure the continuation of critical FVRS functions.

Recommendation: The Department should conduct testing of the FVRS Disaster Recovery Plan at least annually pursuant to Rule and Department Policy.

Finding 4: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to data and IT resources that promote an appropriate separation of duties and that restrict users to only those functions necessary for their assigned job duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, or destruction.

As noted in the Background section of this report, Bureau of Voter Registration Services staff within the Department enter data into the FVRS through the use of the Voter Focus application. We reviewed the access privileges of 42 Voter Focus accounts including user and system administrator accounts as of February 4, 2015. Our review disclosed the following:

- 14 user accounts had update access privileges in Voter Focus that were inappropriate for the users' assigned job duties.
- 3 system administrator accounts were unnecessary and not required for performing system administration functions as Department staff could not determine their original creation dates, uses, or purposes.

In response to our audit inquiry, Department management indicated that full administrative access privileges or a combination of update and inquiry access privileges could be assigned in Voter Focus but that the ability to assign inquiry-only access privileges was not available in the Department's version of Voter Focus. Department management further indicated that the ability to assign inquiry-only access privileges in Voter Focus would require the Department to request a program change from the Voter Focus IT vendor. Notwithstanding the limitation of assigning inquiry-only access privileges in Voter Focus, inappropriate and unnecessary access privileges increase the risk of unauthorized disclosure, modification, or destruction of data and IT resources.

Recommendation: The Department should take steps to ensure that access privileges of Voter Focus accounts are commensurate with users' assigned job duties and are necessary.

Finding 5: Database Change Management

Effective change controls over modifications to the database help ensure that only authorized, tested, and approved database changes are implemented into the production database environment. The effectiveness of database change controls is enhanced through post-implementation mechanisms that provide reasonable assurance that all database changes implemented into the production database environment have been processed through appropriate authorization, testing, and approval controls.

Although the Department used forms and project-tracking tools in the change control process to authorize, test, and approve the FVRS database changes before the changes were implemented into the FVRS production database environment, the Department had not established a post-implementation mechanism, such as the use of system-generated logs or a reconciliation process, to provide reasonable assurance that all database changes implemented into the FVRS production database environment followed the change control process.

Without a post-implementation mechanism to ensure that all database changes to the FVRS production database environment followed the established change control process and were authorized, tested, and approved, the risk is increased that erroneous or unauthorized database changes may be implemented into the FVRS production database environment and not be timely detected.

Recommendation: The Department should ensure that a post-implementation mechanism is in place that provides reasonable assurance that all database changes implemented into the FVRS production database environment have gone through the appropriate change control process.

Finding 6: Security Awareness Training

AEIT Rule 71A-1.008(3), Florida Administrative Code, provides that agency workers shall receive initial security awareness training within 30 days of the employment start date. AEIT Rule 71A-1.008(5), Florida Administrative Code, specifies that initial training shall include acceptable use restrictions, procedures for handling exempt, and confidential and exempt information, and computer security incident reporting procedures. Additionally, the Department's *Security Awareness and Training Policy* (*DOSIT- 01-05-14*) states that members of the Department workforce (users) shall receive initial security awareness training within 30 days of the employment start date and prior to accessing confidential information.

Our audit disclosed that, although users signed written acknowledgments that they had received and read certain Department policies and procedures, including security policies, as part of the Department's on-boarding activities, all users hired since July 1, 2014, did not receive security awareness training because the training presentation was not included in the orientation training. Department staff stated that the Department sent, subsequent to our audit inquiry, the security awareness training presentation to all employees hired since July 1, 2014. The lack of timely security awareness training increases the risk that users may inadvertently compromise security.

Recommendation: The Department should strengthen controls to ensure that security awareness training is conducted in a timely manner.

Finding 7: Security Controls - Protection of Confidential and Exempt Data, Software Support, Authentication, Logging, and Separation of Duties

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. This audit disclosed certain Department security controls related to the protection of confidential and exempt data, software support, authentication, logging, and separation of duties that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising FVRS data and related IT resources. However, we have notified

appropriate Department management of the specific issues. Without adequate security controls related to the protection of confidential and exempt data, software support, authentication, logging, and separation of duties, the risk is increased that the confidentiality, integrity, and availability of FVRS data and IT resources may be compromised.

Recommendation: The Department should improve security controls related to the protection of confidential and exempt data, software support, authentication, logging, and separation of duties to ensure the confidentiality, integrity, and availability of FVRS data and IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the findings included in our report No. 2008-187 that were applicable to the scope of this audit.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts 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 from January 2015 through February 2015 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our 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 determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in audit report No. 2008-187 that were applicable to the scope of this audit.

The scope of this audit focused on evaluating selected interface controls applicable to the FVRS during the period July 2014 through February 2015 and selected actions through March 30, 2015. The audit also included selected application-level general controls over security management, contingency planning, logical access to programs and data, and configuration management.

This audit was designed to identify, for the IT system and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of ineffective or inefficient operational policies, procedures, or practices. The focus of this IT operational audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT system and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT system and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

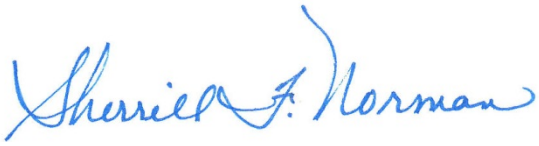
In conducting this audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the IT computing platform for the database.
- Evaluated controls related to FVRS data classification and data ownership.
- Evaluated selected controls regarding valid and unique transactions.
- Evaluated interface processing procedures.
- Obtained an understanding of the key interfaces related to the FVRS.
- Evaluated selected security management controls that included security awareness and other security-related personnel policies.
- Evaluated selected application access controls including authentication controls.
- Obtained an understanding of the procedures for user account management processes for authorizing, creating, modifying, and revoking FVRS user accounts.
- Evaluated the effectiveness of selected logical access controls for the FVRS through Voter Focus to ensure that access privileges were appropriately restricted. Specifically, we reviewed the access privileges of 42 Voter Focus accounts as of February 4, 2015.
- Obtained an understanding of the database configuration management processes.
- Evaluated selected configuration management controls for the FVRS.
- Evaluated FVRS performance and capacity monitoring controls.
- Evaluated FVRS IT maintenance controls.

- Evaluated selected contingency planning and disaster recovery controls for the FVRS.
- Evaluated the adequacy of FVRS logging controls.
- Evaluated selected procedures for the protection of confidential and exempt data.
- Evaluated selected software support procedures.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report on pages 9 through 12.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of this IT operational audit.



Sherrill F. Norman, CPA
Auditor General

FLORIDA DEPARTMENT of STATE

RICK SCOTT
Governor

KEN DETZNER
Secretary of State

June 17, 2015

David W. Martin, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

RE: Preliminary and Tentative audit findings and recommendations on Information Technology (IT) Operational Audit of the Department of State, Florida Voter Registration System (FVRS)

Dear Mr. Martin:

Please accept this letter and attachment as the Department's response to your letter dated May 18, 2015 applicable to the audit referenced above.

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

Sincerely,

Ken Detzner
Secretary of State

R. A. Gray Building • 500 South Bronough Street • Tallahassee, Florida 32399
Telephone: (850) 245-6500 • Facsimile: (850) 245-6125 www.dos.state.fl.us
Commemorating 500 years of Florida history www.fla500.com

PRELIMINARY AND TENTATIVE AUDIT FINDINGS RESPONSE

Finding No. 1: Department FVRS IT maintenance controls needed improvement.

Recommendation: The Department should improve FVRS IT maintenance controls to include appropriate documentation of maintenance schedules, maintenance records, and routine analyses of maintenance records.

Agency Response:

In addition to the processes in current use, the Department implemented a series of additional processes to record maintenance. The process details the extent of the maintenance, the timeframe, and signoff by management.

Finding No. 2: Department FVRS performance and capacity monitoring controls needed improvement.

Recommendation: The Department should improve FVRS performance and capacity monitoring controls.

Agency Response:

The Department is migrating to a new platform in July 2015. A baseline will be established on the new platform. This baseline will determine metrics that will be monitored and documented on a monthly basis. The Department will compare past, current, and future database performance and capacity data to ensure optimal efficiency of the FVRS database.

Finding No. 3: Although the Department had a Disaster Recovery Plan (Plan) in place for the FVRS, the Plan had not been tested since April 2011.

Recommendation: The Department should conduct testing of the FVRS Disaster Recovery Plan at least annually pursuant to Rule and Department Policy.

Agency Response:

The Department has tested every step of the current disaster recovery process except for taking the production database offline. It is imperative that the production system for FVRS is active at all times. The Department is migrating to a new hardware platform in July 2015. The set up for the new platform will not require the production system to be down during disaster testing. Once the new hardware is in place, the Department will annually conduct testing of the Disaster Recovery Plan pursuant to Rule and Department Policy.

Finding No. 4: Some inappropriate and unnecessary access privileges existed in the Voter Focus application that is used to enter data into the FVRS.

Recommendation: The Department should take steps to ensure that access privileges of Voter Focus accounts are commensurate with users' assigned job duties and are necessary.

Agency Response:

The Department recognizes the limitations of the current Voter Focus application. The 14 users that are referenced will have the use of the Voter Focus application added to their job duties. For access to data in FVRS, the Department relies upon an annual outside vendor license which serves as the interface application. Only two levels of access currently exist in that program: a) Full administrative and b) Inquiry/update. All assigned users involve staff in confidential or managerial positions and have had a level 1 or level 2 background check as a matter of employment. The Department is currently undergoing a major rewrite of FVRS in which the ability to restrict access privileges to inquiry-only will become a part of a system.

Finding No. 5: The Department had not established a mechanism to provide reasonable assurance that all changes implemented into the FVRS production database environment were properly authorized, tested, and approved.

Recommendation: The Department should ensure that a post implementation mechanism is in place that provides reasonable assurance that all database changes implemented into the FVRS production database environment have gone through the appropriate change control process.

Agency Response:

The Department created a change management control document. This document provides reasonable assurance that all database changes implemented into the FVRS production database are properly authorized, tested, and approved. Additionally, the Department will use system logging to ensure that only authorized, tested, and approved changes were made to the database.

Finding No. 6: Security awareness training for members of the Department workforce hired since July 1, 2014, had not been conducted in a timely manner.

Recommendation: The Department should strengthen controls to ensure that security awareness training is conducted in a timely manner.

Agency Response:

All newly-hired employees are provided with a copy of the Department's IT Security policies and procedures, as well as a copy of the PowerPoint training, so they are aware of IT security protocols at the commencement of their employment with the agency. A written acknowledgement is required and placed in the file. Although employees

received the policies, a limited number of employees during the audit period had not received the PowerPoint. This issue was addressed and the Department has strengthened controls.

Finding No. 7: Certain Department security controls related to protection of confidential and exempt data, software support, authentication, logging, and separation of duties needed improvement.

Recommendation: The Department should improve security controls related to the protection of confidential and exempt data, software support, authentication, logging, and separation of duties to ensure the confidentiality, integrity, and availability of FVRS data and IT resources.

Agency Response:

The Department has implemented improved security controls related to protection of confidential and exempt data, software support, authentication, logging, and separation of duties to ensure the confidentiality, integrity, and availability of FVRS data and IT resources.