

STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

DEPARTMENT OF STATE

Voting System Standards and Certification,
Voter Registration Records Maintenance,
Selected Administrative Activities,
and Prior Audit Follow-Up



Sherrill F. Norman, CPA
Auditor General

Secretary of State

The Department of State is established by Section 20.10, Florida Statutes. The head of the Department is the Secretary who is appointed by the Governor and subject to confirmation by the Senate. During the period of our audit, the following individuals served as Secretary of State:

Laurel Lee From February 4, 2019
Michael Ertel January 8, 2019, through January 24, 2019
Ken Detzner Through January 8, 2019

The team leader was Robin Ralston, CPA, and the audit was supervised by Samantha Perry, CPA.

Please address inquiries regarding this report to Samantha Perry, CPA, Audit Manager, by e-mail at samanthaperry@aud.state.fl.us or by telephone at (850) 412-2762.

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

FLAuditor.gov

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

Voting System Standards and Certification, Voter Registration Records Maintenance, Selected Administrative Activities, and Prior Audit Follow-Up

SUMMARY

This operational audit of the Department of State (Department) focused on voting system standards and certification, voter registration records maintenance, and selected administrative activities. The audit also included a follow-up on applicable findings noted in our report Nos. 2017-195 and 2014-181. Our audit did not disclose any widespread irregularities or pervasive errors in the voter registration records nor significant reportable issues in the voting system standards and certification process; however, we did identify areas for improvement regarding voter registration records maintenance. Our audit disclosed the following:

Voter Registration Records Maintenance

Finding 1: Department controls over voter registration records maintenance need enhancement to better identify duplicate registrations and registrations for deceased voters and convicted felons, and to ensure that potential voter registration record errors are appropriately investigated and corrected, as necessary.

Finding 2: Department controls for ensuring that persons who register or preregister to vote satisfy statutory age requirements and for analyzing the reasonableness of the recorded dates of birth for voters need improvement.

Finding 3: Department records did not always evidence the timely receipt of forms from county Supervisors of Elections certifying that voter address and voter registration records maintenance activities were conducted in accordance with State law nor evidence Department review of such forms.

Information Technology Controls

Finding 4: Department information technology (IT) access privilege controls for the Voter Focus application, the Bureau of Voter Registration Services Application, and the Department network need enhancement.

Finding 5: Department configuration management controls need improvement to ensure that Department records evidence the authorization, review, testing, and approval of IT system changes.

Finding 6: Contrary to the State of Florida *General Records Schedule GS1-SL for State and Local Government Agencies* retention requirements, the Department did not retain access control records related to the disablement of network access privileges.

Finding 7: Certain security controls related to network user authentication need improvement to ensure the confidentiality, integrity, and availability of Department data and IT resources.

Help America Vote Act

Finding 8: The Department did not adequately evaluate the Supervisors of Elections' risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the subawards

associated with the 2018 Help America Vote Act Election Security Grants. Additionally, the Department did not correctly identify certain Federal award information to the Supervisors of Elections in the subaward agreements.

Selected Administrative Activities

Finding 9: Department controls over mobile device assignment, use, and disposal and for the retention of text messages in accordance with State law need improvement.

Finding 10: Security controls over mobile device utilization need improvement to ensure the confidentiality, integrity, and availability of Department data and IT resources.

Finding 11: Department controls over the administration of Florida Single Audit Act requirements need improvement.

Finding 12: As similarly noted in our report No. 2017-195, Department controls over employee access to the Florida Accounting Information Resource Subsystem need improvement to reduce the risk of unauthorized disclosure, modification, or loss of Department data.

Finding 13: Department controls need improvement to ensure that purchasing cards are only used for authorized transactions in accordance with State law, purchasing card transactions are timely approved, and purchasing card activity is promptly reconciled to supporting records.

Finding 14: The Department did not always timely cancel purchasing cards upon a cardholder's separation from Department employment. Additionally, Department controls for monitoring the reasonableness of purchasing cardholder assignments and timely conducting cardholder status reviews need improvement.

Finding 15: As similarly noted in prior audit reports, most recently in our report No. 2017-195, the Department did not always timely record property acquisitions to Department property records. In addition, the Department did not timely reconcile physical inventory results to the property records, accurately record all property information in Department property records, or appropriately depreciate capital assets in accordance with Department of Financial Services guidance.

Finding 16: The Department had not established policies and procedures for the surplus IT equipment data sanitization and disposal process, nor did Department records evidence the specific surplus IT equipment sanitized and disposed of by a vendor.

Finding 17: Museum of Florida History and Knott House Museum controls were not always sufficient to effectively safeguard moneys collected. A similar finding related to the Museum of Florida History was noted in our report No. 2017-195.

BACKGROUND

The primary functions of the Department of State (Department) are to collect the State's important public records, preserve the State's rich historical and cultural heritage, promote economic development through a business-friendly corporate filing environment, facilitate public access to State Government, and provide oversight to ensure fair and accurate elections. To execute its mission, the Department is organized into the Office of the Secretary and six divisions: the Division of Administration, Division of

Corporations, Division of Cultural Affairs, Division of Elections, Division of Historical Resources, and Division of Library and Information Services. To perform these functions, the Legislature appropriated approximately \$101.7 million to the Department for the 2018-19 fiscal year and authorized 408 positions.¹ For the 2019-20 fiscal year, the Legislature appropriated \$128.9 million to the Department and authorized 408 positions.²

FINDINGS AND RECOMMENDATIONS

VOTER REGISTRATION RECORDS MAINTENANCE

The Division of Elections (Division), Bureau of Voter Registration Services (Bureau), coordinates and maintains the Florida Voter Registration System (FVRS) and assists county Supervisors of Elections (Supervisors) with the voter registration and voter removal process. State law³ establishes that Supervisors are to update voter registration information in FVRS, enter new voter registrations into FVRS, and act as the official custodian of documents related to the registration of electors and changes in the voter registration status of electors. State law⁴ specifies that a voter registration application is complete if it:

- Includes the applicant's name; address of legal residence; date of birth; driver's license number, Florida identification card number, or last four digits of the applicant's social security number; the applicant's signature, and
- Affirms the applicant's United States citizenship, that the applicant has not been convicted of a felony or that, if convicted, the applicant had their civil rights restored, and that the applicant had not been adjudicated mentally incapacitated with respect to voting or that, if adjudicated, the applicant had their right to vote restored.⁵

Department staff utilize the Voter Focus application⁶ to access voter registration data in FVRS. According to Department management, a voter's registration record status in FVRS may be, among other things, active, inactive, pre-registered, or removed. A voter's inactive status may be restored to active by the voter updating their registration, requesting a vote-by-mail ballot, or appearing to vote.

According to Department records, the State had 13,409,341 active registered voters as of January 31, 2019. In 2018, 750,353 voter registrations were added and 356,719 voter registrations were removed from the voter registration records.

¹ Chapter 2018-9, Laws of Florida.

² Chapter 2019-115, Laws of Florida.

³ Section 98.015(3), Florida Statutes.

⁴ Section 97.053(5)(a), Florida Statutes (2018).

⁵ Pursuant to Chapter 2019-162, Laws of Florida, Section 97.053(5)(a), Florida Statutes, was amended to require the applicant to confirm that they had not been convicted of a felony or that, if convicted, the applicant had their civil rights restored through executive clemency or their voting rights restored pursuant to Article VI, Section 4 of the State Constitution.

⁶ The Sarasota County Supervisor of Elections did not utilize Voter Focus as its local voter registration support system during the period of our audit.

Finding 1: Maintenance of Voter Registration Records

State law⁷ and Department rules⁸ require the Department and the Supervisors to protect the integrity of the electoral process by ensuring the maintenance of accurate and current voter registration records. The Department is responsible for performing voter registration records maintenance activities, including identifying the following for removal from the voter rolls: (1) duplicate registrations; (2) deceased persons; (3) those adjudicated mentally incapacitated with respect to voting and who have not had their voting rights restored; and (4) those who have been convicted of a felony and whose rights have not been restored. The Department utilizes the Bureau of Voter Registration Services Application (BVRSA) to perform voter registration records maintenance activities and provides the results of the activities to the Supervisors for voter registration information to be updated in FVRS in accordance with Department rules.

The Department reviews new registration records daily to identify potential duplicate registrations. Additionally, the Department reviews registration records for duplicate registrations if a demographic change is made to an existing voter record. Upon identification of a potential duplicate registration, the Department is to notify the applicable Supervisors to review and resolve the identified issue. According to Department procedures, at least three demographics were required to identify potential duplicate registrations: voter's last name, birth date, and either the last four digits of the voter's social security number, the voter's first name, or the voter's driver's license number. The BVRSA identifies potential duplicate registration matches and sends automated voter match notifications to the applicable Supervisors. The Supervisors were required to review the identified potential duplicate registrations and record a determination of the voter's status in FVRS within 2 weeks of receiving the information from the Department.⁹

The Department identifies registration records for deceased voters daily by comparing demographic information in FVRS to demographic information in death records received from the Department of Health (DOH) and the United States Social Security Administration (SSA). Additionally, the Department identified¹⁰ registration records for voters convicted of a felony charge who have not received clemency by daily comparing FVRS demographic information to information maintained by Clerks of the Circuit Courts, the Board of Executive Clemency, the Department of Law Enforcement, and the Department of Corrections (DOC). According to Department procedures, to identify potential deceased persons, at least three demographics were required through DOH matches and at least four demographics were required through SSA matches. At least three demographics were required to identify convicted felons. Possible demographic matches included the voter's last name, first name, birth date, address, last four digits of the voter's social security number and, for convicted felons, their driver's license number. The BVRSA sends an automated match notification to the Supervisors for review of death record matches where the

⁷ Section 98.075(1), Florida Statutes.

⁸ Department Rule 1S-2.041, Florida Administrative Code.

⁹ Department Rule 1S-2.041(4)(a)4., Florida Administrative Code.

¹⁰ Effective for the period July 2017 through January 2019. An amendment to Article VI, Section 4 of the State Constitution allowed for any disqualification from voting arising from a felony conviction to terminate and voting rights be restored upon completion of all terms of the offender's sentence. Effective February 14, 2019, the Department suspended providing unconfirmed felony matches to the Supervisors and then resumed the match process on June 7, 2019.

last name, first name, birth date, and last four digits of the voter's social security number in FVRS matched DOH death records. For all other matches, Department staff were to assess the validity of the matches and send potential valid matches to the Supervisors. State law¹¹ requires the Supervisors to remove from FVRS the names of deceased registered voters within 7 days of receiving the match information from the Department and to remove the names of voters convicted of a felony after notifying the voters of their potential ineligibility in accordance with the procedures outlined in State law.¹²

To determine whether the Department performed voter registration records maintenance activities in accordance with State law, Department rules, and Department policies and procedures, we performed inquiries of Department management, reviewed Department policies and procedures, and examined Department records for 40 voter registration records maintenance activities (10 duplicate registrations, 10 deceased persons registrations, 10 adjudicated mentally incapacitated persons registrations, and 10 convicted felons registrations) performed during the period July 2017 through January 2019. We also analyzed Department voter registration records to identify potential duplicate registrations and compared Department registration records to DOH death records and DOC convicted felon records to determine whether the Department appropriately identified deceased voters and convicted felons through the registration records maintenance activities. Our audit procedures found that Department policies and procedures did not require Department staff to follow up with Supervisors to ensure that, as necessary, the Supervisors removed voters identified through the Department's voter registration records maintenance process or require potential voter record errors to be investigated and corrected, as warranted, by Department or Supervisor staff. These deficiencies may have contributed to some of the issues noted on audit, including:

- **Duplicate registrations** Our examination of Department voter registration maintenance activity records for the period July 2017 through January 2019 for voters with a recorded social security number disclosed 103 instances where the Department identified potential duplicate voter registration records. Our evaluation of 10 of these voter registration records matches disclosed that the applicable Supervisors determined the matches to be invalid; however, 2 of the matches identified the same voter's last name, first name, middle name, social security number, and date of birth.

Our analysis of Department voter registration records disclosed 58 instances previously unidentified by the Department where the last name, first name, middle name, social security number, and date of birth of an active or inactive voter was identified in two registration records. In response to our inquiry regarding our evaluation of 13 of these potential duplicate registration records, Department management indicated that some of the matches were not identified due to non-demographic changes to the voters' registration records and that such changes do not initiate an automated check for duplicate records.

Additionally, we identified another instance of a potential duplicate voter registration record that the Department had not previously identified where the voter's first name, last name, and birth date were identified in two registration records. According to Department management, the Supervisor revised the voter's status from removed to active and, because the status revision was not a demographic change, the duplicate record was not identified by the Department. We also noted two instances where the Department identified the duplicate matches; however, as of September 10, 2019, the matches had been in a pending status for more than 3 and 8 years,

¹¹ Section 98.075(3) and (5), Florida Statutes.

¹² Section 98.075(7), Florida Statutes.

respectively. While both voter records remained active, our review of Department records disclosed no voting history for either voter. In response to our audit inquiry, Department management indicated that the applicable Supervisor was responsible for updating the status.

- **Deceased voters** Our examination of Department voter registration maintenance records for the period July 2017 through January 2019 for voters with a recorded social security number disclosed 122 instances where the Department identified potential deceased voter registration records. Our evaluation of 10 of these matches disclosed that the Department sent 6 of the voter registration records to the applicable Supervisor. However, the Supervisors responded, on the same day the records were received from the Department, that 5 of the matches were invalid, although 4 of the voters' last names, first names, and social security numbers matched DOH death records and the first name and social security number of the fifth voter matched the death records. For the sixth match, the Supervisor indicated that the match was valid but did not remove the voter from the voter registration records until 312 days after the voter's death and subsequent to our audit inquiry.

Our evaluation of the 10 matches also found that, although 3 of the voter registration records matched on last name, first name, and social security number and 1 matched on last name and social security number between FVRS and DOH death records, the Department marked the matches as invalid. Subsequent to our audit inquiry, and between 241 and 576 days from the dates the individuals died, the Department referred the records to the Supervisors and the voters' records were removed from FVRS. In all 4 instances, Department records disclosed that no votes were recorded for the individuals in elections subsequent to their death. According to Department management, the matched records were not appropriately determined valid and timely referred to the Supervisors due to employee error.

In addition, our comparison of FVRS voter registration records for the period July 2017 through January 2019 to DOH death records for deaths occurring prior to January 31, 2019, disclosed 295 instances previously unidentified by the Department where the social security number and last name of an active or inactive voter in the registration records matched the social security number and last name of the individual in the DOH death records. Our evaluation of 10 of these matches disclosed that, for 7 voter registrations, the first name in the registration record and death record matched, and for another registration, the first name did not match due to an obvious misspelling. Our examination of the voting records for the 10 voters disclosed that a vote was cast in the name of one voter in a general election 33 days after the voter's recorded date of death and in two other elections, 166 and 222 days after the voter's recorded date of death. For another voter, voting records indicated that a vote was cast by mail in a general election 219 days after the voter's recorded date of death. According to Department management, although the last name, first name, and social security number matched the DOH death records, because the birth dates of the 10 voters did not match between the registration records and death records, the recorded information did not meet the matching criteria.

- **Convicted felons** Our comparison of FVRS voter registration records for the period July 2017 through January 2019 to DOC convicted felon records for inmates or probationers who had a sentence entered with an admission date on or prior to May 13, 2019, disclosed 3,005 instances previously unidentified by the Department where the social security number and last name of an active or inactive voter in the registration records matched the social security number and last name of an individual in the convicted felon records. Our evaluation of 10 of the matches disclosed that:
 - In 9 instances, the date of birth also matched between the voter registration record and the convicted felon record and in the other instance, the date of birth varied by exactly 1 year.
 - In 7 instances, the first name also matched in the voter registration record and the convicted felon record and in the other 3 instances, the first name did not match due to an obvious misspelling.

Our examination of Department records for the 10 voters disclosed that 8 had voted in an election. Of those 8, 3 voters had been granted clemency by the Florida Commission on Offender Review prior to their voting date. Based on the information available for audit, we could not determine the other 5 voter's eligibility to vote. In response to our audit inquiry, Department management indicated that the matches were not identified for 9 of the 10 voters because the necessary convicted felon records data was not available to the Department for a match and, for the other voter, the first name recorded in FVRS did not match the first name in the DOC records.

The establishment of policies and procedures for Department monitoring of the Supervisors' handling of voter registration records maintenance information provided by the Department for review and follow up and effective procedures for identifying duplicate, deceased, and convicted felon voter registration records are necessary for the Department, in coordination with the Supervisors, to maintain accurate and current voter registration records and ensure and demonstrate that only eligible persons are permitted to vote.

Recommendation: We recommend that Department management establish policies and procedures to monitor the Supervisors' handling of voter registration records maintenance, including the correction of registration records when warranted. We also recommend that Department management:

- **Strengthen voter registration records maintenance activity controls to better account for non-demographic voter record changes.**
- **Appropriately identify all potential duplicate, deceased, and convicted felon voter registration records.**
- **Take appropriate action to promote the integrity of the State's voter registration records.**

Finding 2: Registration Records Accuracy

State law¹³ specifies that a person may become a registered voter only if that person is a citizen of the United States, a legal resident of the State of Florida, a legal resident of the county in which that person seeks to be registered, and is at least 18 years of age. A person who is otherwise qualified may preregister to vote on or after his or her 16th birthday and, after the preregistered voter turns 18, the Supervisors update the preregistered voter's status to active and the voter may vote in an election. The voter's name and date of birth is to be subject to verification by the Department through a data exchange with the Department of Highway Safety and Motor Vehicles' Driver and Vehicle Information Database, or through self-attestation in instances where the voter has not been issued a driver's license or identification card.

To ensure that only eligible persons can vote in elections or preregister to vote, it is necessary that accurate information be recorded in FVRS voter registration records. As part of our audit, we evaluated FVRS records as of January 31, 2019, and identified 901 (856 active and 45 inactive) voter registration records where the individuals appeared to have pre-registered to vote prior to their 16th birthday. Our examination of 26 of the 856 active voter registration records disclosed that some individuals who preregistered to vote, or became an active registered voter, did not meet the applicable age requirement. Specifically:

¹³ Section 97.041(1), Florida Statutes.

- At the time of preregistration, the initial recorded dates of birth for 17 individuals indicated that they were at least 16 years old and eligible to preregister to vote. However, according to Department management, subsequent to the individuals' voter registration status becoming active, the Supervisors revised the individuals' dates of birth in FVRS to later dates. Based on the revised birth dates, the 17 individuals had preregistered to vote when they were 14 or 15 years of age. Additionally, 14 of the 17 individuals were between 16 and 17 years old when their voter registration status changed from preregistered to active.
- Another individual's voter registration status became active when the voter was 17. In response to our audit inquiry, Department management indicated that the applicable Supervisor changed the registration status from preregistered to active 8 days before the voter turned 18.

According to Department records, none of these 18 individuals voted in an election prior to their 18th birthday.

Our analysis of FVRS voter registration records as of January 31, 2019, also disclosed 9,901 active and 1,783 inactive voters between the ages of 100 and 144, of which 386 were active voters older than 110. Our examination of the FVRS registration records for 18 of the 11,684 voters and inquiries of Department management disclosed that:

- The Department had identified 4 active voters as potential matches to DOH death records; however, the Supervisors determined the matches to be invalid. According to Department management, the matches were determined to be invalid because there was no driver's license information in FVRS for these voters that would enable the Supervisors to confirm the date of birth.
- 2 active voters were 130 and 144 years old based on their recorded birth dates. In response to our audit inquiry, Department management indicated that the voters' birth dates were incorrectly recorded and the voters were actually 30 and 44 years of age.
- The Department had not identified potential data entry or other errors in the recorded birth dates of 5 active and 7 inactive voters whose ages, based on those birth dates, ranged from 105 to 133.

According to Department management, the Department implemented logical data analysis procedures to identify voters whose dates of birth may be incorrect or voters who may be deceased but were not identified through the DOH and SSA death record matches. However, based on the results of our audit, the effectiveness of Department controls for ensuring the accuracy of voter registration records and that such records support the eligibility of persons registered or pre-registered to vote in accordance with State law was not always apparent.

Recommendation: To ensure the accuracy of voter registration records and that such records support the eligibility of persons registered or pre-registered to vote in accordance with State law, we recommend that Department management strengthen age-based logical data analysis procedures and work with the Supervisors to address issues, if any, identified by the procedures.

Finding 3: Voter Address List and Registration Records Maintenance Certifications

State law¹⁴ requires each Supervisor to certify to the Department by January 31 and July 31 of each year that the Supervisor conducted voter address list maintenance activities and voter registration records maintenance activities during the first and second 6 months of the year. If, based on the certifications

¹⁴ Sections 98.065(6)(a) and 98.075(8), Florida Statutes.

required in State law, the Department determines that a Supervisor has not satisfied the maintenance requirements, the Department is to satisfy the certification requirements for the Supervisor. Failure to conduct the voter address list and voter registration records maintenance activities constitutes a violation of the State Election Code.¹⁵

Department rules¹⁶ require the Supervisor certifications to be made on a *Certification of Address List Maintenance Activities* (Address List) form and a *Certification of Voter Registration Records Maintenance Activities* (Registration Records) form. Department procedures¹⁷ required the Bureau to collect Address List and Registration Records forms from each Supervisor and forward the forms to the Department Legal Office for review. Forms could be submitted to the Bureau by mail, e-mail, or fax. According to Bureau management, the receipt date for forms received by mail was to be evidenced by a date stamp, forms received by e-mail by the e-mail date, and for forms received by fax, the fax date or a date stamp.

As part of our audit, we interviewed Bureau management and examined records related to the Address List form and Registration Records form submitted by 20 counties for one of the certification periods ended July 31, 2017, January 31, 2018, or July 31, 2018, to determine whether the Department timely received the forms from Supervisors and whether the Department reviewed the forms to verify that the Supervisors conducted voter address and voter registration records maintenance activities in accordance with State law. Our audit procedures disclosed that Bureau management did not maintain a log to track the receipt or review of the Address List and Registration Records forms. In addition, Bureau management indicated that, contrary to Department procedures, the Bureau no longer forwarded the forms to the Department Legal Office for review. Instead, Bureau management indicated that the forms were reviewed by the Bureau administrative assistant, although documentation evidencing such reviews was not available. We also noted that Department procedures did not require Bureau staff to log the date that the forms were received or document the review of the forms. Subsequent to our audit inquiry, the Department prepared a log to evidence the dates forms are received and management indicated that controls for tracking the forms had been enhanced to include the dates the forms were received and reviewed.

Documentation evidencing the timely receipt and review of Address List and Registration Records forms from all Supervisors would provide the Department greater assurance that voter address and voter registration records maintenance activities are conducted in accordance with State law. Such documentation would also enhance the Department's ability to identify instances where the Department would be required to satisfy the certification requirements specified in State law.

Recommendation: We recommend that Department management enhance controls to ensure that adequate documentation evidencing the timely receipt and review of Address List and Registration Records forms from all Supervisors is maintained in Department records.

¹⁵ Chapter 97-106, Florida Statutes.

¹⁶ Department Rules 1S-2.041(3)(g)(3) and (4)(e)(2), Florida Administrative Code.

¹⁷ Department *BVRS Procedures Manual*, Chapter 16: *Registration Records Maintenance*.

State law¹⁸ requires State agencies to establish information security controls to ensure the security of agency data, information, and information technology (IT) resources. Additionally, Agency for State Technology (AST)¹⁹ rules²⁰ established minimum security standards for ensuring the confidentiality, integrity, and availability of State agency data, information, and IT resources. As part of our audit, we evaluated selected IT controls for the FVRS, Voter Focus, BVRSA, and the Department network.

Finding 4: IT Access Privilege Controls

AST rules²¹ required State agencies to periodically review user access privileges for appropriateness and to ensure that IT access privileges were removed when access to an IT resource was no longer required. Prompt action to remove access privileges is necessary to help prevent misuse of the access privileges. AST rules²² also required all users be granted access to agency IT resources based on the principles of least privilege and separation of duties. Department policy²³ required all requests for activating and deactivating user access to IT services or systems be logged in an official call tracking system. According to Department management, submitting and logging user access requests was accomplished by completing an Access Control Form and submitting it through the Department's ticketing system, Revelation.

According to Department records, as of May 1, 2019, there were 43 active Voter Focus user accounts, including 12 system administrator accounts (8 user accounts and 4 service accounts) and, as of March 27, 2020, there were 28 active BVRSA user accounts, including 6 security administrator accounts. Additionally, during the period July 2017 through January 2019, the Department had 457 user accounts with access to the Department's network. As part of our audit, we evaluated Voter Focus, BVRSA, and Department network access controls, reviewed Department procedures, and examined Department records to determine whether user access privileges were appropriately granted based on the principles of least privilege and separation of duties, periodically reviewed for appropriateness, and timely disabled upon an employee's separation from Department employment or when access privileges were no longer required. Our audit procedures disclosed that Department IT access privilege controls need enhancement. Specifically, we noted that:

- Department procedures did not require, and the Department could not provide documentation evidencing, the conduct of periodic reviews of user access privileges for Voter Focus, BVRSA, and the Department's network during the period July 2017 through January 2019. Additionally, Department procedures did not provide guidance for using the Access Control Form to request

¹⁸ Section 282.318(4)(d), Florida Statutes.

¹⁹ Effective July 1, 2019, Chapter 2019-118, Laws of Florida, created the Division of State Technology (DST) within the Department of Management Services (DMS) and transferred the existing powers, duties, functions, personnel, records, property, and funds of the Agency for State Technology (AST) to the DST. Effective July 1, 2020, the DST was abolished, and the Florida Digital Service was established in its place.

²⁰ AST Rule, Chapter 74-2, Florida Administrative Code. Effective July 1, 2019, AST Rules, Chapter 74-2, Florida Administrative Code, were transferred to DMS Rules, Chapter 60GG-2, Florida Administrative Code. AST Rules, Chapter 74-2, Florida Administrative Code, were in effect during our audit period (July 2017 through January 2019).

²¹ AST Rule 74-2.003(1)(a), Florida Administrative Code.

²² AST Rule 74-2.003, Florida Administrative Code.

²³ Department Policy DOSIT-01-06-14, *Access Controls Policy*.

user access privileges be disabled. Consequently, the Department did not disable Voter Focus system administrator access privileges when no longer required. In response to our audit inquiries, Department management identified 5 of the 12 system administrator accounts (3 user accounts and 2 service accounts) as obsolete and indicated that the 5 accounts would be disabled.

- The Department inappropriately granted to four Voter Focus service accounts the capability to create user accounts. Additionally, a Voter Focus system administrator was assigned incompatible access roles by combining Voter Focus system administration functions with FVRS database administrator functions, and Department procedures did not define system administrator duties or provide guidance for using the Access Control Form to request, approve, and assign user access privileges, including system administrator access privileges. In response to our audit inquiry, Department management indicated that the Department was updating the separation of incompatible duties procedures and that the FVRS database administrator was granted Voter Focus system administrator functions to act as a backup for creating user accounts.

Periodic reviews of user access privileges provide Department management assurance that user access privileges are authorized and remain appropriate. As unauthorized access can occur at any time, timely disabling user access privileges when such privileges are no longer necessary limits the potential for unauthorized disclosure, modification, or destruction of Department data and IT resources by former employees or others. Additionally, appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

Recommendation: We recommend that Department management strengthen IT policies and procedures to ensure that:

- **Periodic reviews of user access privileges are conducted and documented.**
- **User access privileges are timely disabled upon a user's separation from Department employment or when access is no longer needed.**
- **User access privileges are limited to promote an appropriate separation of duties.**

Finding 5: Configuration Management Controls

To promote effective configuration management over IT resources, AST rules²⁴ required State agencies to establish a configuration management control process to manage upgrades and modifications to existing IT resources. Effective configuration management controls ensure that all configuration changes (program or functionality changes) follow a configuration management process that provides for an appropriate separation of duties and ensures changes are appropriately authorized, reviewed, tested, and approved. Additionally, agency records should clearly document and track the configuration management process from initial authorization to final approval of the change. Department policy²⁵ required the Department to implement a change management process for modifications to production IT resources and a patch management process for IT resources.

According to Department records, the Department completed 11 FVRS configuration changes, including 2 emergency programming changes and 1 BVRSA configuration change during the period July 2017 through January 2019. To determine whether the FVRS and BVRSA changes were appropriately

²⁴ AST Rule 74-2.003(5)(c), Florida Administrative Code.

²⁵ Department *Network and Systems Operational Security Policy*.

authorized, reviewed, tested, and approved, we requested Department records for 4 FVRS changes, including the emergency programming changes, and for the BVRSA change. Our audit disclosed that Department records did not always evidence the authorization, review, testing, and approval of FVRS and BVRSA configuration and emergency programming changes and that Department configuration management procedures need enhancement. Specifically, we noted that:

- Department records for 2 FVRS configuration changes did not evidence the authorization, review, testing, and approval of the changes.
- Department records for the BVRSA configuration change did not evidence the authorization, review, and approval of the change. Additionally, while the Department provided documentation evidencing that some testing had occurred, the documentation did not evidence that final testing had been completed.
- Department records for the 2 FVRS emergency programming changes did not evidence Department approval. Additionally, for one of the emergency changes, Department records did not evidence that testing had been conducted and, for the other emergency change, Department records did not evidence that the change had been reviewed or that final testing had been completed.
- Department procedures did not provide guidance for executing change and patch management processes or require documentation to support the configuration management process.

According to Department management, IT system changes could be requested by completing an IT Maintenance System Change form or using Revelation. However, Department management indicated that approvals for system changes had to be provided via e-mail, as neither the IT Maintenance System Change form nor Revelation provided a complete set of system change management approvals. Additionally, Department management indicated that the Department application systems development and maintenance process, including procedures for emergency changes, was being updated.

Adequate procedures for executing change and patch management processes and for retaining documentation evidencing, for each system change, the entire configuration management process provides assurance that only properly authorized, reviewed, tested, and approved changes were made.

Recommendation: We recommend that Department management strengthen IT policies and procedures to ensure that Department records evidence the entire configuration management process for each system change.

Finding 6: Records Retention

The State of Florida *General Records Schedule GS1-SL for State and Local Government Agencies* (General Records Schedule) specifies that access control records for employees, contractors, or subscribers must be retained for 1 year after superseded or access rights are deactivated. However, we noted that the Department only retained system-generated network access control records related to the disablement of access privileges for 90 days. Although we requested, Department management was unable to provide an explanation for not retaining the required network access control records for 1 year.

Absent the appropriate retention of system-generated network access control records, the risk is increased that the Department may not have sufficient documentation to assist in future investigations of security incidents, should they occur.

Recommendation: We recommend that Department management ensure that system-generated network access control records are retained in accordance with the General Records Schedule.

Finding 7: Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that certain security controls related to network user authentication need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and related IT resources. However, we have notified appropriate Department management of the specific issues.

Without appropriate security controls related to network user authentication, the risk is increased that the confidentiality, integrity, and availability of Department data and related IT resources may be compromised.

Recommendation: We recommend that Department management improve certain security controls related to network user authentication to ensure the confidentiality, integrity, and availability of Department data and related IT resources.

HELP AMERICA VOTE ACT

Pursuant to Section 101 of the Help America Vote Act (HAVA), in April 2018 the Department was awarded a \$19,187,003 Federal grant²⁶ to “improve the administration of elections for Federal office, including to enhance election technology and make election security improvements” to the systems, equipment, and processes used in Federal elections. To improve the administration and security of elections throughout the State, the Department subgranted HAVA funds to each Supervisor. The Supervisors were to apply to the Department for funds by July 18, 2018, and expend the funds by November 6, 2018. As shown in **EXHIBIT A** to this report, the subgrant amounts ranged from \$55,386 to \$1,644,919, and totaled \$15,450,000.

Finding 8: HAVA Grant Administration

Federal regulations²⁷ require the Department, as the grantee, to evaluate each Supervisor’s (subrecipient’s) risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the subgrant (subaward) to determine the appropriate subrecipient monitoring. The grantee must monitor the activities of the subrecipient as necessary to ensure that the subaward is used for authorized purposes, in compliance with Federal statutes, regulations, and the terms and conditions of the subaward, and that subaward performance goals are achieved. Federal regulations specify that subrecipient monitoring must include reviewing financial and performance reports required by the grantee and following up and ensuring that subrecipients take timely and appropriate action on all deficiencies detected through audits, on-site reviews, and other means. Additionally, Federal regulations²⁸ require the Department to ensure that every subaward is clearly identified to the subrecipient as a subaward at

²⁶ Catalog of Federal Domestic Assistance No. 90.404 – 2018 HAVA Election Security Grants.

²⁷ Title 2, Section 200.331(b), Code of Federal Regulations.

²⁸ Title 2, Section 200.331(a), Code of Federal Regulations.

the time of the subaward and include certain Federal award information, such as the Catalog of Federal Domestic Assistance (CFDA) number and CFDA name. To facilitate compliance with Federal regulations, the Department utilized a standard subaward agreement for all HAVA subrecipients which included Federal award information and required subrecipients to submit a final expenditure report with supporting documentation evidencing allowable expenses by November 30, 2018.

As part of our audit, we inquired of Department management and examined Department records to determine whether the Department administered the HAVA grant in accordance with Federal regulations. Our audit procedures disclosed that:

- The Department did not adequately evaluate subrecipient risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the subaward. According to Department management, the Supervisors were determined to be low risk subrecipients because they are constitutional officers; however, the Department did not complete a risk assessment to support this determination. Although the Department required Supervisors to submit financial expenditure reports, absent an adequate evaluation of subrecipient risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the subaward, Department records did not evidence that subrecipients were appropriately monitored based on a risk assessment and that subaward performance goals were achieved.
- The Department's subaward agreements with the Supervisors did not include the correct CFDA number or CFDA name due to employee oversight. The failure to notify subrecipients of the correct award information may result in subrecipient noncompliance with Federal regulations.

Recommendation: We recommend that Department management enhance controls to ensure that all Federal awards are administered in accordance with applicable Federal requirements, including those requiring an evaluation of subrecipient risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the subaward and correct identification of Federal award information in subaward agreements.

SELECTED ADMINISTRATIVE ACTIVITIES

As part of our audit, we evaluated selected Department administrative activities and controls, including those related to mobile devices, the administration of the Florida Single Audit Act, Florida Accounting Information Resource Subsystem (FLAIR) access privileges, purchasing cards, property, and revenue collections.

Finding 9: Mobile Devices

The Department utilizes mobile devices, such as cellular telephones, smartphones, tablets, and mobile Internet hotspot devices, to execute its statutory responsibilities. Department of Financial Services (DFS) guidelines²⁹ specify that State agencies are to establish internal controls over the use of State-owned or leased cellular telephones to ensure that related payments serve an authorized public purpose. The guidelines and Department policy³⁰ further specified that billing options should be reviewed to determine that the most economical option is selected, considering the specific usage requirements of the cellular telephone user. Pursuant to Department policy, each month, employees assigned a mobile device were

²⁹ DFS Reference Guide for State Expenditures.

³⁰ Department Cellular Telephone Usage Policy.

to review the Department's mobile device bill, identify all personal calls, sign and complete a *Monthly Cellular Telephone Invoice Review* form (Review form) certifying the extent of personal usage, and pay within 30 days for personal calls totaling more than \$1.

Department policy³¹ also established standards for managing, securing, and tracking Department-owned mobile devices. To promote the appropriate disposal of mobile devices, it is important to follow an orderly and controlled disposal process that includes controls for properly safeguarding mobile devices before disposal and removing (sanitizing) sensitive and confidential information from the devices.

As noted in Finding 6, State law³² requires the Department to maintain public records in accordance with the records retention schedule³³ established by the Department, Division of Library and Information Services. The schedule specifies that the retention periods for electronic communications, including text messages, are based on the content, nature, and purpose of the messages. Some of the purposes include administrative correspondence (3 fiscal years), program and policy development correspondence (5 fiscal years), and transitory messages, which are to be maintained until obsolete, superseded, or administrative value is lost.

During the period July 2017 through January 2019, the Department expended \$38,619 for mobile devices and related services and, as of January 2019, had 87 Department-owned mobile devices. As part of our audit, we evaluated Department controls over mobile device assignment, use, disposal, and the retention of text messages to determine whether the Department had established adequate controls related to the use of Department-owned mobile devices. We noted that:

- The Department did not maintain a list of Department-owned mobile devices assigned to employees.
- The Department did not always obtain monthly personal usage certifications from employees assigned a Department-owned mobile device. Our examination of the Department's November 2018 mobile devices invoice and Department records found that 12 of 33 applicable employees did not complete a Review form evidencing the extent of personal usage and required reimbursement amounts. Additionally, the Review forms for the other 21 employees were not signed until March 2019. According to Department management, the Department was behind in collecting the Review forms and reimbursements due to staff turnover.
- The Department did not review the billing options for or the necessity of vacant (unassigned) Department-owned mobile devices. During the period March 2018 through February 2019, the Department paid charges totaling \$1,786 for 15 unassigned mobile devices. Additionally, while maintaining services for those mobile devices, the Department purchased 5 additional mobile devices for new employees. In response to our audit inquiry, Department management indicated that Department policies and procedures did not require a periodic review of mobile device assignments and plans nor had management designated a mobile devices administrator to conduct such reviews.
- Department procedures did not adequately ensure that Department-owned mobile devices were returned to the Department upon an employee's separation from Department employment or that devices returned were unlocked, enabling the Department to identify the mobile devices and process the devices for future use or disposal. Specifically, the Department could not locate 7 of

³¹ Department *Mobile Devices Policy*.

³² Section 119.021(2)(b), Florida Statutes.

³³ State of Florida *General Records Schedule GS1-SL for State and Local Government Agencies*.

15 mobile devices assigned to employees who separated from Department employment during the period November 2018 through February 2019. Additionally, while Department management indicated that the other 8 mobile devices had been disposed of, records evidencing their disposal could not be provided for audit. According to Department management, when an employee separated from Department employment, the employee's supervisor was to complete an Employee Separation Checklist (Checklist) and notate whether a mobile device was collected from the employee. However, Department management indicated that supervisors did not always utilize the Checklist and that the absence of a designated mobile devices administrator may have also contributed to the issues noted on audit.

- The Department had not established sanitization procedures for Department-owned mobile devices and did not track the number of devices requiring sanitization prior to disposal. Consequently, Department records did not evidence that mobile devices were sanitized prior to disposal.
- The Department did not retain text messages in accordance with State law and the State's records retention schedule. According to Department management, text messaging capabilities were to be blocked on all Department-owned mobile devices. However, our examination of Department records disclosed that 12 Department employees sent or received 258 text messages during the period July 2018 through February 2019. In response to our audit inquiry, Department management indicated that the text messaging function was inadvertently enabled on some mobile devices. Subsequent to our audit inquiry, Department management indicated that the text messaging setting on all mobile devices had been reviewed and disabled.

Effective controls for managing the assignment and use of Department-owned mobile devices would reduce the risk that the Department may incur unnecessary mobile device charges and that mobile devices may be used for unauthorized purposes. In addition, reviewing billing options for unassigned mobile devices, appropriately accounting for all devices, and establishing procedures for sanitizing mobile devices prior to disposal would strengthen Department management's ability to obtain the most economical mobile device plans and protect the confidentiality and integrity of Department data and resources. Absent the retention of text messages in accordance with State law, the Department's ability to provide access to public records is diminished.

Recommendation: We recommend that Department management designate a mobile devices administrator responsible for the management of the Department's mobile device program. We also recommend that Department management enhance mobile device controls, including mobile device policies and procedures, to ensure that:

- Department records evidence all Department-owned mobile devices assigned to employees.
- Monthly personal usage certifications are obtained from all employees assigned a Department-owned mobile device.
- Mobile device assignments and plans are periodically reviewed by the mobile devices administrator for appropriateness and cost-effectiveness.
- Mobile devices are returned to the Department upon an employee's separation from Department employment.
- Department records evidence the sanitization of mobile devices prior to disposal.
- Any text messages are retained in accordance with State law and the State's records retention schedule.

Finding 10: Mobile Device Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to mobile device utilization need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department management of the specific issues.

Without appropriate security controls related to the use of mobile devices by Department employees and contractors, the risk is increased that the confidentiality, integrity, and availability of Department data and IT resources may be compromised.

Recommendation: We recommend that Department management enhance certain security controls related to employee and contractor use of mobile devices to ensure the confidentiality, integrity, and availability of Department data and IT resources.

Finding 11: Florida Single Audit Act

State Financial Assistance (SFA) is financial assistance provided from State resources to non-State entities to carry out a State project and is to be administered in accordance with the requirements of the Florida Single Audit Act (FSAA),³⁴ DFS rules,³⁵ and Rules of the Auditor General.³⁶ The purpose of the FSAA, among other things, is to establish uniform State audit requirements for non-State entities receiving SFA, promote sound management of SFA, and ensure State agency monitoring, use, and follow-up on audits of SFA.

The FSAA requires each non-State entity that expends \$750,000 or more of SFA in any fiscal year to obtain a State single audit or a project specific audit conducted by an independent auditor. Upon completion of the audit, an SFA recipient is to provide the State awarding agency and the Auditor General a copy of the entity's Financial Reporting Package (FRP).³⁷ Among other things, the FRP is to address the recipient's compliance with State project requirements, any deficiencies in internal controls, and the amount of SFA expended by the recipient in conducting the State project. In addition, the FSAA specifies that State awarding agencies are to review each recipient's FRP to determine whether timely and appropriate corrective action had been taken with respect to audit findings and recommendations.

Department policies and procedures³⁸ required grant managers to include in all SFA recipient grant award agreements standard FSAA language requiring a recipient to submit an FRP to the Department within 9 months of the end of the recipient's fiscal year and monitor SFA recipients for compliance with grant guidelines and grant award agreement terms. Department policies and procedures³⁹ also required the

³⁴ Section 215.97, Florida Statutes.

³⁵ DFS Rules, Chapter 69I-5, Florida Administrative Code.

³⁶ Chapters 10.550 and 10.650, Rules of the Auditor General.

³⁷ An FRP includes the recipient's financial statements, Schedule of Expenditures of State Financial Assistance, auditor's report, management letter, auditee's written responses or corrective action plan, and correspondence on follow-up on prior corrective actions taken.

³⁸ Department *Grants Policies and Procedures* Version 2.0, dated May 2018.

³⁹ Department *Independent Audit Report Review Process*, dated July 2018.

Department, Office of the Inspector General (OIG), to review the FRPs using a Single Audit Review Tracking Sheet (Tracking Sheet) that listed the date FRPs were received and reviewed and what, if any, actions were needed to address audit findings. The OIG determined which SFA recipients were required to submit an FRP to the Department using grant disbursement data from the DFS Florida Accountability Contract Tracking System (FACTS). Grant managers also sometimes provided grant expenditure information to the OIG.

According to Department records, the Department provided SFA in excess of \$87.3 million to 937 non-State entities during the period July 2017 through January 2019. As part of our audit, we reviewed Department FSAA policies and procedures and examined selected recipient FRPs and related SFA records to determine whether the Department obtained and reviewed recipient FRPs in accordance with FSAA requirements. Our audit procedures disclosed that:

- The Department's process for identifying the non-State SFA recipients required to submit an FRP did not adequately ensure that the Department obtained and reviewed all required FRPs. Specifically, our analysis of the 2017-18 fiscal year Tracking Sheet disclosed that 12 county SFA recipients were not included on the Tracking Sheet. Consequently, the Department did not obtain or review FRPs for 10 of the counties that received SFA from the Department totaling \$3,888,538 for the fiscal year ended September 30, 2017. According to Department management, the grant managers relied on the OIG to track recipient compliance with the FSAA reporting requirements. Department management also indicated that SFA recipients may have been omitted from the Tracking Sheet because the FACTS grant disbursement data did not always include the information needed to accurately identify which recipients met the FSAA threshold and were required to submit an FRP and because grant managers did not consistently provide grant expenditure information. In such cases, the OIG was only able to determine whether the recipients had met the FSAA threshold if the recipients submitted an FRP.
- The Department did not always follow up on instances of recipient noncompliance with FRP filing requirements. Specifically, we noted that 576 of the 607 FRPs recorded as received by the Department during the period July 2017 through January 2019 were received 2 to 425 days (an average of 239 days) after the FRPs were due. In response to our audit inquiry, Department management indicated that the Department had not established a centralized location for recipients to submit their FRPs to ensure that all FRPs were timely obtained and reviewed.
- As of March 19, 2019, the OIG had not completed the review of 6 FRPs included on the Tracking Sheet as being received in July and August 2018. According to OIG management, the FRPs were not timely reviewed due to employee oversight.

Established processes that promote compliance with the FSAA and provide for proper State project oversight help ensure that SFA will be properly administered in compliance with the FSAA and applicable rules. Further, without the timely receipt and appropriate review of FRPs, any recipient noncompliance or control deficiencies noted on audit may not be timely followed up on and resolved.

Recommendation: We recommend that Department management enhance FSAA oversight processes to ensure that all non-State entities required to submit an FRP to the Department are accurately identified, FRPs are timely obtained and reviewed by the OIG, and identified instances of recipient noncompliance or other deficiencies are timely followed up on and resolved.

Finding 12: FLAIR Access Controls

The Department utilizes FLAIR to authorize the payment of Department obligations and to record and report financial transactions. Controls over employee access to FLAIR are necessary to help prevent and detect improper or unauthorized use of FLAIR access privileges. AST rules⁴⁰ required State agencies to specify that all users be granted access to agency IT resources based on the principles of least privilege and separation of duties. AST rules⁴¹ also required State agencies to ensure that IT access privileges are removed when access to an IT resource is no longer required and to periodically review user access privileges for appropriateness.

Department policies and procedures⁴² required FLAIR access privileges to be reviewed at the beginning of each quarter. In addition, according to Department management, supervisors were to complete and send to the IT access control custodian an Access Control Form (Access Form) when an employee separated from Department employment. The Access Form was to list all IT access privileges to be removed and, if FLAIR access privileges were listed, the IT access control custodian was to forward the Access Form to the FLAIR Administrator to remove the former employee's access privileges.

In our report No. 2017-195 (Finding 8), we noted that Department controls over employee access to FLAIR needed improvement. As part of our follow-up audit procedures, we evaluated Department FLAIR access controls and again noted that Department controls were not always effective to ensure the appropriateness of FLAIR user access privileges or the timely removal of access privileges. Specifically, we noted that:

- Employees performing financial management functions had been granted update capabilities to incompatible functions in FLAIR. Our examination of March 2019 FLAIR access control records for 48 active FLAIR user accounts assigned to 47 Department employees disclosed that:
 - 7 user accounts had update capabilities to both the disbursement and vendor client functions.
 - 6 user accounts had update capabilities to both the cash receipts and disbursement functions.
 - 6 user accounts had update capabilities to both cash receipts and accounts payable functions.
 - 6 user accounts had update capabilities to both accounts receivable and accounts payable functions.
 - 5 user accounts had update capabilities to both fixed assets accounting and fixed assets custodial functions.

According to Department management, Department policies and procedures for reviewing FLAIR access privileges did not specifically consider the assignment of incompatible access privileges.

- FLAIR user access privileges were not always timely removed upon an employee's separation from Department employment. Our examination of FLAIR access control and People First⁴³ records disclosed that FLAIR access privileges for 4 of the 10 Department employees with FLAIR access privileges who separated from Department employment during the period July 2017 through January 2019 remained active 7 to 29 business days (an average of 16 business days) after the employees' separation dates. In response to our audit inquiry, Department management

⁴⁰ AST Rule 74-2.003, Florida Administrative Code.

⁴¹ AST Rule 74-2.003(1)(a)(6) and (8), Florida Administrative Code.

⁴² Department *Access Control Review Procedure*, dated April 2018.

⁴³ People First is the State's human resource information system.

indicated that the Access Form did not list specific IT systems and, since the supervisors did not specify the removal of FLAIR access privileges on the Access Forms, the IT access control custodian was unaware of the need to communicate to the FLAIR Administrator the need to remove the employees' access privileges.

- The Department did not review the appropriateness of FLAIR user access privileges during the period July 2017 through January 2019, as no employee was assigned to conduct such reviews.

The effective separation of incompatible financial management duties, prompt removal of FLAIR user access privileges upon an employee's separation from Department employment, and periodic reviews of employee access privileges reduce the risk of unauthorized disclosure, modification, or loss of Department data.

Recommendation: We recommend that Department management enhance controls to ensure the appropriate assignment and timely removal of FLAIR user access privileges. Such enhancements should include:

- Limiting FLAIR user access privileges to promote an appropriate separation of duties.
- Revising the Access Form to specify the IT system access privileges to be removed upon an employee's separation from Department employment.
- Removing FLAIR user access privileges immediately upon an employee's separation from Department employment.
- Periodically reviewing the appropriateness of FLAIR user access privileges.

Finding 13: Purchasing Card Transactions and Reconciliations

As a participant in the State's purchasing card program, the Department is responsible for implementing key controls, including procedures for approving and monitoring purchasing card transactions and timely processing purchasing card transactions. According to Department policy,⁴⁴ cardholders were to submit original receipts for each transaction to their Division approver within 1 business day of purchase, Division approvers were to review and approve transactions within 3 calendar days of purchase, and the Department was to reimburse the State's purchasing card vendor within 10 calendar days of receiving a charge. According to the Department's *Purchasing Card Program Agency Plan* (Agency Plan), the Bureau of Planning, Budget, and Financial Services (Bureau) was responsible for reconciling within 15 days of the end of each month cardholder receipts and supporting documentation to purchasing card activity reports.

We analyzed Department purchasing card transactions, examined Department records, and evaluated the adequacy of Department purchasing card controls and noted that Department controls could be enhanced to promote appropriate card usage and the timely processing of transactions and reconciliation of purchasing card activity to source records. Specifically:

- During the period February 2018 through January 2019, the Department used a purchasing card to acquire background screening services with costs totaling \$42,774 for Department employees. However, contrary to State law,⁴⁵ the Department did not evidence the purchase of these services by a written agreement or purchase order. As a result of using a purchasing card to acquire the

⁴⁴ Department *Cardholder Purchasing Card Program Policy*, dated March 2013.

⁴⁵ Section 287.058(4), Florida Statutes.

services, the Department incurred a 3 percent surcharge totaling \$1,107. Although we requested, Department management was unable to provide an explanation for using a purchasing card to acquire the background screening services. However, Department management agreed that a purchase order should have been used rather than a purchasing card.

- The Department did not timely process purchasing card transactions. Our examination of Department data found that, during the period July 1, 2017, through January 31, 2019, the Department reimbursed the State's purchasing card vendor late for 3,064 purchasing card charges, totaling \$694,484. Specifically, the vendor was reimbursed 11 to 210 calendar days (an average of 27 calendar days) after the purchasing card charges were received. Additionally, as of January 31, 2019, 12 purchasing card charges, totaling \$4,163, had been outstanding for 16 to 99 calendar days (an average of 38 calendar days). In response to our audit inquiry, Department management indicated that the purchasing card transactions were not timely processed because cardholders did not timely submit receipts for approval.
- The Department did not timely reconcile cardholder receipts to purchasing card activity reports. Our examination of Department records disclosed that 664 of the 998 reconciliations performed during the period July 2017 through January 2019 were completed 1 to 314 calendar days (an average of 53 calendar days) late. Additionally, as of March 2019, the Department had not completed 7 other reconciliations due during the period April 2018 through January 2019. According to Department management, the reconciliations were not timely completed due to cardholder delays in submitting purchasing card receipts for approval and delays in processing purchasing card transactions.

Without effective controls to ensure the proper use of purchasing cards, the risk is increased that Department purchases may result in unnecessary surcharges and may not comply with State law. Additionally, timely processing purchasing card charges and timely reconciling purchasing card activity to supporting records would provide Department management greater assurance that purchasing card use is subject to appropriate monitoring and purchasing card activity is in accordance with Department management's expectations and the requirements of the State purchasing card program.

Recommendation: We recommend that Department management strengthen purchasing card oversight controls to ensure that purchasing cards are only used for transactions in accordance with State law, purchasing card transactions are timely approved, and purchasing card activity is promptly reconciled to supporting records.

Finding 14: Purchasing Card Controls

Controls for approving the issuance of purchasing cards and timely canceling purchasing cards upon a cardholder's separation from Department employment or when an employee no longer requires a purchasing card to perform his or her job duties promote the appropriate administration of the State's purchasing card program. According to the Department's Agency Plan, the Purchasing Card Program Administrator (PCPA) was responsible for issuing and canceling purchasing cards and for conducting quarterly cardholder status reviews for compliance with Agency Plan requirements. As of January 2019, the Department had 129 active purchasing cards and purchasing card charges totaled \$981,472 during the period July 2017 through January 2019.

As part of our audit, we examined Department purchasing card records and evaluated the adequacy of Department controls for purchasing card issuances, activity, and cancellations during the period July 2017 through January 2019. Our audit procedures disclosed that Department purchasing card controls needed improvement. Specifically, we noted that:

- The Department did not timely cancel the purchasing cards for 3 of the 28 cardholders who separated from Department employment during the period July 2017 through January 2019. Specifically, the purchasing cards were canceled 2, 5, and 56 business days after the cardholders' employment separation dates. In response to our audit inquiry, Department management indicated that the PCPA did not timely deactivate 2 of the purchasing cards due to oversight and was not timely notified of the other cardholder's separation from Department employment. Although our audit tests did not disclose any charges incurred subsequent to the cardholders' separation from Department employment, timely cancellation of purchasing cards upon a cardholder's separation from Department employment reduces the risk that unauthorized purchases will be made.
- As of January 31, 2019, no charges had been made on 11 of the 129 active purchasing cards for periods ranging from 1 to 2.5 years. Consequently, these cardholders may not have required a purchasing card for the performance of their job duties. Subsequent to our audit inquiry, in March 2019, Department management deactivated 3 of the 11 purchasing cards and indicated that the remaining purchasing cards were needed by the cardholders to perform their job responsibilities. Absent effective controls to periodically monitor the necessity of purchasing card assignments, the risk of unauthorized purchasing card use is increased.
- The Department did not perform quarterly cardholder status reviews in accordance with the Agency Plan. Our examination of Department records disclosed that the Department did not complete cardholder status reviews for the quarters ended September 2017, December 2017, March 2018, June 2018, and September 2018. Additionally, the cardholder status review for the quarter ended December 2018 was not initiated until 53 days after the quarter end and was not completed until 74 days after the end of the quarter. In response to our audit inquiry, Department management indicated that the reviews were not performed or timely performed due to staff vacancies. Controls to timely review the status of cardholders for compliance with Agency Plan requirements would promote the effective administration and use of Department purchasing cards.

Recommendation: We recommend that Department management promptly cancel purchasing cards upon a cardholder's separation from Department employment and strengthen procedures to ensure the periodic monitoring of the continued need for purchasing card assignments. We also recommend that Department management take steps to ensure the timely completion of cardholder status reviews.

Finding 15: Property Management

Effective controls for the management of tangible personal property⁴⁶ require that property items be adequately controlled, safeguarded, and accounted for by Department management. DFS rules⁴⁷ require State agencies to record all tangible personal property in the FLAIR Property Subsystem and that, for Statewide financial reporting purposes, such property items are to be capitalized. DFS guidance⁴⁸

⁴⁶ During the period of our audit (July 2017 through January 2019), tangible personal property was defined in applicable laws and rules as State-owned equipment, fixtures, and other tangible personal property of a nonconsumable or nonexpendable nature, the value or cost of which was \$1,000 or more and the projected useful life of which was 1 year or more. Effective July 1, 2020, DFS Rule 69I-72.002, Florida Administrative Code, was amended to increase the tangible personal property threshold to \$5,000.

⁴⁷ DFS Rule 69I-72.002, Florida Administrative Code.

⁴⁸ Chief Financial Officer Memorandum No. 05 (2011-2012), *Statewide Financial Statements Capital Asset Guidance and Rules for Tangible Personal Property*.

specified that capital assets, including furniture and equipment valued at or greater than \$1,000⁴⁹ and buildings and building improvements valued at or greater than \$100,000 were to be capitalized and depreciated over their estimated useful life, beginning with the month that the asset was received by the agency. Additionally, DFS rules⁵⁰ require the Department to complete a physical inventory of all tangible personal property at least once each fiscal year. Upon completion of a physical inventory, the results are to be reconciled to Department property records and noted differences are to be investigated and corrected, as appropriate.

Department procedures⁵¹ specified that all attractive property items (e.g., cameras and laptop computers) with a value or cost of less than \$1,000 were to be recorded in Department property records. Department procedures required that, for each property item purchased, Department staff complete a Property Receipt Form to document, among other things, the property received date, location, and the finance and property custodians. The Property Receipt Form was to be used by the Department Property Custodian to establish the property record in the FLAIR Property Subsystem. The Department was to add property items to Department property records within 60 days after payment for the item.

According to Department property records, as of January 31, 2019, the Department was responsible for 1,770 active property items with acquisition costs totaling approximately \$25 million. Of those items, 275 items with acquisition costs totaling approximately \$667,967 were purchased during the period July 2017 through January 2019. As part of our audit, we evaluated Department property management procedures and examined Department property records to determine whether the procedures promoted, and the records evidenced, the timely and accurate recording of property in Department property records. Our audit procedures disclosed that:

- As similarly noted in prior audit reports, most recently in our report No. 2017-195 (Finding 7), the Department did not always timely update Department property records for property acquisitions. Our examination of Department records disclosed that, as of January 31, 2019, 37 property acquisition transactions, totaling \$182,815, remained in a pending status and the items had not been added to Department property records, although 78 to 566 calendar days (an average of 286 calendar days) had elapsed since the transactions were made.

In addition, we examined Department records for the 275 property items acquired during the period July 2017 through January 2019 and noted that the Department had not timely added 26 of the property items, with acquisition costs totaling \$79,581, to Department property records. The 26 property items were added to Department property records 63 to 116 calendar days (an average of 94 calendar days) after the items were received. In response to our audit inquiry, Department management indicated that the property items were inadvertently overlooked when adding property items to Department records.

- The Department did not always accurately record property received dates in Department property records. Our examination of Department records for 25 property items, with acquisitions costs totaling \$220,869, acquired during the period July 2017 through January 2019, disclosed that the received dates recorded in Department property records for 18 of the items, with acquisition costs totaling \$26,360, were not the received dates indicated on the Property Receipt Forms. According to Department management, incorrect dates were recorded due to employee error.

⁴⁹ Effective July 1, 2020, Chief Financial Officer Memorandum No. 13 (2020-2021) increased the Statewide financial reporting capitalization threshold for furniture and equipment to \$5,000.

⁵⁰ DFS Rule 69I-72.006, Florida Administrative Code.

⁵¹ Department *Property Procedures*.

- The Department did not timely reconcile the results of the 2017-18 fiscal year inventory to Department property records. While the physical inventory was completed in June 2018, the results of the inventory were not reconciled to Department property records until February 2019. Our review of Department procedures found that, while the procedures addressed the physical inventory process, the procedures did not specify a time frame for reconciling physical inventory results to Department property records.
- The Department did not always accurately record the condition of property items in Department property records. Specifically, our analysis of Department property records as of January 31, 2019, found that 1,733 of the 1,770 property items were recorded as “new” although 992 of the property items were acquired between 1970 and 2013. In addition, Department records did not include a condition for 31 other property items. In response to our audit inquiry, Department management indicated that the Department had not established a process to evaluate the condition of property items and that the condition field was not updated due to employee oversight.
- The Department did not appropriately depreciate capital assets. Our analysis of Department property records found that the Department did not depreciate 73 furniture and equipment property items, with acquisition costs totaling \$264,382, although the items met the \$1,000 capitalization threshold.⁵² According to Department management, the 73 furniture and equipment property items were not depreciated due to employee oversight. Additionally, because Department procedures directed staff to depreciate all property items, regardless of the capitalization threshold, the Department depreciated 562 furniture and equipment property items and buildings and building improvements, with total acquisition costs totaling \$562,890, that did not meet the applicable capitalization thresholds established in DFS guidance.

Absent effective property controls, Department management has reduced assurances regarding the accuracy of the information needed to correctly report and maintain proper accountability over Department property and cannot demonstrate compliance with applicable DFS rules and guidance.

Recommendation: We recommend that Department management strengthen controls to ensure that Department property records are timely and accurately updated for property acquisitions. We also recommend that Department management enhance property management procedures to promote the accurate recording of each property item’s condition in the property records, the timely reconciliation of physical inventory results to Department property records, and the depreciation of capital assets in accordance with DFS guidance.

Finding 16: Surplus IT Equipment Sanitization and Disposition Documentation

In performing their assigned duties, Department employees routinely access confidential and sensitive data, such as voter social security numbers. Effective security controls include established policies and procedures for proper data sanitization and disposal of surplus IT equipment (i.e., computers, disks, servers, and other equipment or media) containing confidential and sensitive data. Additionally, the Department should maintain complete and accurate records documenting the data sanitization and IT equipment disposal process.

The Department utilized a vendor to sanitize and dispose of surplus IT equipment with data storage capabilities and obtained from the vendor a Certificate of Data Destruction and Recycling as evidence that the sanitization and disposal process had been completed. According to Department records, during the period July 2017 through January 2019, the Department disposed of 103 items identified as surplus

⁵² The acquisition cost for 10 of the 73 items was over \$5,000 and totaled \$126,454.

IT equipment with data storage capabilities, including computers, printers, scanners, Ethernet switches, and servers.

We reviewed Department policies and procedures and examined property disposition records and noted that, while the Department had established policies and procedures addressing property management and the disposal of surplus property, the policies and procedures did not address the Department's IT equipment data sanitization and disposition process. Additionally, we noted that the Certificate of Data Destruction and Recycling did not include sufficient information, such as manufacturer, model, and serial number, to identify the specific surplus IT equipment that had been sanitized and disposed of. In response to our audit inquiry, Department management indicated that the Certificate of Data Destruction and Recycling was the only documentation of the sanitization and disposition process required to be provided by the vendor.

Effective policies and procedures for managing the surplus IT equipment data sanitization and disposition process help promote accountability and reduce the risk that Department data may be compromised. Without complete records evidencing the specific surplus IT equipment sanitized and disposed of, Department management lacks the information necessary to ensure proper accountability for and control over surplus IT equipment and any confidential or sensitive information contained therein.

Recommendation: We recommend that Department management establish policies and procedures for the surplus IT equipment data sanitization and disposal process. We also recommend that Department management work with the vendor to ensure Department records adequately evidence the sanitization and disposition of each surplus IT equipment item.

Finding 17: Collection Safeguards

Appropriate safeguards for moneys collected are essential for the prevention and detection of theft or loss. Such safeguards include logging collections, documenting any transfers of collections between employees, and timely depositing all moneys received. The Museum of Florida History (Museum) and the Knott House Museum (Knott House) collect revenue from a variety of sources, including donation boxes, membership dues, individual contributions, and parking fees.

Museum policies and procedures⁵³ specified that the Museum Administrative Assistant was to restrictively endorse checks received by mail and log the checks into an electronic Master Log and on a paper Collection Log sheet. For Knott House donation box and education program collections, a Knott House employee and the Education Program Supervisor were to count the collections weekly, log the collections on a Collection Log sheet, and sign the Collection Log. Knott House collections were to be transferred to the Museum Administrative Assistant for logging into the Master Log. At least every 2 weeks, the Museum Administrative Assistant and the Museum Development Director were to count Museum donation box collections and log the information on a Collection Log sheet. The Knott House and Museum collections were to be given to the Museum Gift Shop Manager who was to prepare a bank deposit, stamp the Collection Log sheet as received for deposit, initial the Collection Log, and take the deposit to the bank. The Museum Development Director was to record the collection information into

⁵³ Museum of Florida History and Friends of the Museums of Florida History, Inc., *Financial Management Policy and Procedures Manual*.

Museum accounting records. After the collections were deposited, the bank receipt was provided to another gift shop employee to verify the deposit and initial the deposit form.

During the period July 2017 through January 2019, the Museum and Knott House collected revenues totaling \$207,323. In our report No. 2017-195 (Finding 6), we noted that Museum controls were not always sufficient to effectively safeguard moneys collected. As part of our follow-up audit procedures, we evaluated the implementation of Museum and Knott House policy and procedure requirements for collecting, processing, depositing, recording, and safeguarding Museum and Knott House cash gifts and other receipts and examined Museum and Knott House records for 30 deposits, composed of 220 cash and check collections, totaling \$121,844, made during the period July 2017 through January 2019. Our audit procedures found that:

- Collection Log sheets did not include 15 checks totaling \$10,306 and, as a result, Museum records did not evidence that the checks were appropriately transferred or timely deposited. In response to our audit inquiry, Museum management indicated that the checks may have not been logged due to vacancies in the Museum Development Director and Museum Administrative Assistant positions.
- For 61 cash and check collections totaling \$48,937, Museum and Knott House records did not evidence the Museum Gift Shop Manager's initials and date documenting the transfer of collections from the Museum Administrative Assistant or Knott House. Additionally, for 13 cash collections totaling \$591 and 2 check collections totaling \$2,025, the collections were not included on the Master Log evidencing the transfer from Knott House staff to the Museum Administrative Assistant. According to Museum management, staff turnover and vacancies may have contributed to the issues noted on audit.
- 58 cash and check collections totaling \$11,979 were deposited 15 to 58 calendar days (an average of 34 calendar days) after the transactions were logged. According to Museum management, competing staff priorities may have been a factor in the delays.

Effective collection controls would provide greater assurance that Museum and Knott House cash and check collections are appropriately safeguarded and accounted for and that any theft or loss, should it occur, will be timely detected.

Recommendation: We recommend that Museum management strengthen controls over Museum and Knott House collections to ensure the logging of all check and cash collections, recording of collections transfers, and the timely deposit of funds.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the applicable findings included in our report Nos. 2017-195 and 2014-181.

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 operational audit from February 2019 through April 2020 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.

This operational audit of the Department of State (Department) focused on voting system standards and certification, voter registration records maintenance, and selected administrative activities. The overall objectives of the audit were:

- To evaluate management's performance in establishing and maintaining internal controls, including controls designed to prevent and detect fraud, waste, and abuse, and in administering assigned responsibilities in accordance with applicable laws, administrative rules, contracts, grant agreements, and other guidelines.
- To examine internal controls designed and placed in operation to promote and encourage the achievement of management's control objectives in the categories of compliance, economic and efficient operations, the reliability of records and reports, and the safeguarding of assets, and identify weaknesses in those internal controls.
- To determine whether management had corrected, or was in the process of correcting, all applicable deficiencies disclosed in our report No. 2014-181 (Findings 1 through 5).
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

Our audit also included steps to determine whether management had corrected, or was in the process of correcting, all applicable deficiencies noted in our report No. 2017-195 (Findings 4 through 8).

This audit was designed to identify, for those programs, activities, or functions 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 inefficient or ineffective operational policies, procedures, or practices. The focus of this 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 transactions, legal compliance matters, records, and controls considered.

As described in more detail below, for those programs, activities, and functions included within the scope of our 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 our audit; obtaining an understanding of the program, activity, or function; 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 our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of transactions and records. Unless otherwise indicated in this report, these transactions and records 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 vendors, and as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit, we:

- Reviewed applicable laws, rules, Department policies and procedures, and other guidelines, and interviewed Department personnel to obtain an understanding of Department voting system standards and certification and voter registration records maintenance controls.
- Obtained an understanding of selected Department information technology (IT) controls, assessed the risks related to those controls, evaluated whether selected general and application IT controls for the Florida Voter Registration System (FVRS), the Voter Focus application, the Bureau of Voter Registration Services Application, and the Department's network were in place, and tested the effectiveness of the selected controls.
- Examined documentation for the two applications submitted to the Department for voting system certification during the period July 2017 through January 2019 to determine whether the Department adequately documented the voting system examinations and timely approved or disapproved of the voting system in accordance with Sections 101.5605, 101.5606, and 101.5607, Florida Statutes, and Department Rule 1S-2.015, Florida Administrative Code.
- Interviewed Department personnel, evaluated the Department's process for requesting reimbursement from vendors that submit applications for voting system certification, and examined travel reimbursement documentation related to the two applications for voting system certification submitted to the Department during the period July 2017 through January 2019 to determine whether the Department sought and received reimbursement from the vendors in accordance with Section 101.5605(2)(b), Florida Statutes.
- Interviewed Department personnel and examined Department records related to the two applications for voting system certification submitted to the Department during the period July 2017 through January 2019 to determine whether Department records evidenced that the Secretary of State and all voting system examiners did not have any pecuniary interest in the voting systems equipment.
- Interviewed Department personnel, evaluated Department policies and procedures, and examined Department records to determine whether the Department had established a process to update and maintain an accurate inventory of county voting systems in accordance with Section 101.5607, Florida Statutes.
- From the population of 83 voting system acquisition requests made by 49 counties to the Department during the period July 2017 through January 2019:
 - Examined Department records for 10 selected voting system acquisition requests to determine whether the Department tracked the timeliness of county voting system acquisition request filings.
 - Compared 10 selected voting system acquisition requests to the Department's voting system inventory records to determine whether the Department accurately updated the voting system inventory records for the requests and whether the Department appropriately notified the counties that had satisfied their acquisition filing requirements.
- Interviewed Department personnel, evaluated Department policies and procedures, and examined Department records to determine whether the Department had established a process

to effectively review county voting system security procedures and to timely resolve noted deficiencies.

- From the population of 54 counties for which the Department conducted a biennial review of the county's security procedures during the period July 2017 through January 2019, examined Department records for 10 selected Department biennial reviews to determine whether the Department had established an effective process to review county voting system security procedures each odd-numbered year, verified compliance with State law and Department rules, and tracked and timely followed up with counties with noted voting system security procedures deficiencies.
- Interviewed Department personnel and examined Department records to determine whether the Department administered the Help America Vote Act grant, totaling \$19,187,003 and awarded in April 2018, in accordance with Federal regulations.
- Interviewed Department personnel, evaluated Department policies and procedures, and examined Department records to determine whether the Department had established a process for identifying and removing from the voter rolls those voters with duplicate registrations, deceased voters, voters adjudicated mentally incapacitated with respect to voting who had not had their voting rights restored, and voters convicted of a felony whose rights had not been restored.
- From the population of 705 registration records maintenance activities for active and inactive voter registration records where the voter had a social security number and the Department identified the voter registration record as having a death match, felon match, or duplicate match in FVRS during the period July 2017 through January 2019, examined Department records for 30 selected registration records maintenance activities to determine whether the Department conducted the registration records maintenance activities in accordance with State law, Department rules, and other applicable guidelines.
- From the population of 2,273 mental incapacity case records received by the Department during the period July 2017 through January 2019, examined Department records for 10 selected mental incapacity case records to determine whether the Department conducted the registration records maintenance activities in accordance with State law, Department rules, and other applicable guidelines.
- Analyzed Department FVRS records as of January 31, 2019, and:
 - Identified potential duplicate voter registrations, selected 30 potential duplicate voter registration record matches, and examined records of Department efforts to detect duplicate voter registration records.
 - Compared the FVRS records to Department of Health death records and identified 295 instances of potential deceased voters. We selected 10 potential deceased voter registration matches and examined records of Department efforts to detect deceased voters.
 - Compared the FVRS records to Department of Corrections records and identified 3,005 instances of potential felon voter registrations. We selected 10 potential felon voter registration records and examined records of Department efforts to detect voters convicted of a felony.
- Analyzed Department FVRS records as of January 31, 2019, and:
 - Identified 856 active and 45 inactive voter registration records where the individuals appeared to have pre-registered to vote prior to their 16th birthday and examined Department records for 26 selected active voter records to determine whether the age at preregistration met the requirements of Section 97.041(1), Florida Statutes.

- Identified 9,901 active and 1,783 inactive voters between the ages 100 and 144 and examined Department records for 18 selected voter records (10 active and 8 inactive) to determine whether the FVRS registration records were accurate.
- From the population of 402 *Certification of Voter Registration Records Maintenance Activities* and *Certification of Address List Maintenance Activities* forms due from 67 County Supervisors of Elections during one of the certification periods ended July 31, 2017, January 31, 2018, and July 31, 2018, examined Department records for selected certifications required for each of 20 selected counties to determine whether the Department obtained and reviewed the 40 selected certifications in accordance with Sections 98.065 and 98.075, Florida Statutes, Department Rule 1S-2.041, Florida Administrative Code, and Department procedures.
- Evaluated Department actions to correct Findings 4 through 8 noted in our report No. 2017-195. Specifically, we:
 - Examined Department policies and procedures to determine whether the policies and procedures required proof of insurance for all outgoing artifact loans and for informing lenders of the provisions of the Florida Arts and Culture Act.
 - Examined Museum of Florida History (Museum) records for the 25 outgoing artifact loans that were in effect during the period July 2017 through January 2019 to determine whether, in making and administering the loans, the Museum obtained adequate proof of insurance in accordance with Department Rule 1T-12.005(5)(c), Florida Administrative Code.
 - Examined Museum records for the 16 incoming artifact loans that were in effect during the period July 2017 through January 2019 to determine whether, in making and administering the loans, the Museum informed the lenders of the provisions of the Florida Arts and Culture Act, in accordance with Section 265.565(3), Florida Statutes.
 - Evaluated the adequacy of Museum and Knott House Museum (Knott House) controls, including policies and procedures, for collecting, processing, depositing, recording, and safeguarding Museum and Knott House cash gifts and other receipt through inquiries of Museum personnel, observations of controls, and examination of relevant records.
 - From the population of 87 deposits for cash and check collections totaling \$207,323 and made during the period July 2017 through January 2019, examined Museum records for 30 selected deposits, totaling \$121,844, to determine whether the collections were timely deposited and properly recorded in Department accounting records. We also observed Department processes for collecting and handling donations prior to deposit.
 - From the population of 275 property items, with costs totaling \$667,967, acquired during the period July 2017 through January 2019, examined Department records for 25 selected property items, with costs totaling \$220,869, to determine whether the Department timely and accurately recorded the property items in Department property records.
 - Interviewed Department personnel to determine whether, during the period July 2017 through January 2019, the Department periodically reviewed the appropriateness of Florida Accounting Information Resource Subsystem (FLAIR) user access privileges.
 - Examined FLAIR access records for the 48 FLAIR user accounts (assigned to 47 Department employees) with update privileges as of March 2019 to determine whether the user accounts had update access privileges to incompatible functions in FLAIR.
 - Examined FLAIR access privileges and People First records for the ten Department employees who separated from Department employment during the period July 2017 through January 2019 and whose FLAIR access privileges were deactivated during the period July 2017 through January 2019 to determine whether the Department timely deactivated user access privileges upon an employee's separation from Department employment.

- Observed, documented, and evaluated the effectiveness of selected Department processes and procedures for:
 - Cash and revenue management activities.
 - The administration of tangible personal property in accordance with applicable guidelines. As of January 2019, the Department was responsible for tangible personal property with related acquisition costs totaling \$25,009,223.
 - The administration of purchasing cards in accordance with applicable guidelines. As of January 31, 2019, the Department had 129 active purchasing cards.
 - The assignment and use of mobile devices with related costs totaling \$38,619 during the period July 2017 through January 2019.
 - The administration of the requirements of the Florida Single Audit Act. During the period July 2017 through January 2019, the Department expended \$87,324,976 for 12 State Financial Assistance programs.
 - The acquisition and management of real property leases in accordance with State law, Department of Management Services rules, and other applicable guidelines. As of February 2019, the Department was responsible for 15 real property leases.
- 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 under the heading **MANAGEMENT'S RESPONSE**.

AUTHORITY

Section 11.45, Florida Statutes, requires that the Auditor General conduct an operational audit of each State agency on a periodic basis. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.



Sherrill F. Norman, CPA
Auditor General

EXHIBIT A

DEPARTMENT ALLOCATION OF HELP AMERICA VOTE ACT ELECTION SECURITY GRANTS

County	Federal Election Activities Funds Total	County	Federal Election Activities Funds Total
Alachua	\$ 216,017	Lee	\$ 457,076
Baker	66,408	Leon	231,112
Bay	157,741	Levy	76,304
Bradford	68,711	Liberty	55,386
Brevard	406,225	Madison	62,294
Broward	1,159,266	Manatee	259,758
Calhoun	59,397	Marion	268,398
Charlotte	162,094	Martin	148,581
Citrus	147,166	Miami-Dade	1,644,919
Clay	165,034	Monroe	100,765
Collier	261,657	Nassau	96,927
Columbia	92,792	Okaloosa	164,820
DeSoto	72,098	Okeechobee	74,865
Dixie	60,856	Orange	766,071
Duval	590,235	Osceola	212,107
Escambia	240,883	Palm Beach	909,513
Flagler	112,678	Pasco	349,347
Franklin	57,832	Pinellas	666,196
Gadsden	78,767	Polk	426,394
Gilchrist	60,881	Putnam	97,077
Glades	58,558	St. Johns	169,525
Gulf	60,865	St. Lucie	226,425
Hamilton	59,718	Santa Rosa	144,159
Hardee	66,398	Sarasota	311,401
Hendry	73,100	Seminole	316,163
Hernando	163,337	Sumter	119,422
Highlands	116,074	Suwannee	76,247
Hillsborough	814,481	Taylor	64,819
Holmes	62,792	Union	60,241
Indian River	141,635	Volusia	378,124
Jackson	82,573	Wakulla	69,501
Jefferson	59,822	Walton	85,740
Lafayette	55,793	Washington	66,046
Lake	242,393		
		Total	<u>\$15,450,000</u>

Source: Department records.

MANAGEMENT'S RESPONSE



FLORIDA DEPARTMENT *of* STATE

RON DESANTIS
Governor

LAUREL M. LEE
Secretary of State

December 22, 2020

Sherrill F. Norman
Auditor General
Claude Denson Pepper Building, Suite G74
111 W. Madison Street
Tallahassee, FL 32399-1540

Dear Ms. Norman:

Enclosed is the Florida Department of State's response to the preliminary and tentative audit findings and recommendations pertaining to the Auditor General's Audit of Voting System Standards and Certification, Voter Registration Records Maintenance, Selected Administrative Activities, and Prior Audit Follow-Up.

If you have any questions, please call Candie Fuller, Interim Inspector General, at 850-245-6195.

Thank you for the opportunity to respond.

Sincerely,


Laurel M. Lee
Secretary of State

Enclosure

c: Candie M. Fuller, Interim Inspector General, DOS
Jennifer Kennedy, Assistant Secretary of State

**R.A. Gray Building • 500 South Bronough Street • Tallahassee, Florida 32399
850.245.6500 • 850.245.6125 (Fax) • DOS.MyFlorida.com**

**Department of State
Response to Preliminary and Tentative Audit Findings
Auditor General Audit
December 22, 2020**

Finding 1: Maintenance of Voter Registration Records

Department controls over voter registration records maintenance need enhancement to better identify duplicate registrations and registrations for deceased voters and convicted felons, and to ensure that potential voter registration record errors are appropriately investigated and corrected, as necessary.

Recommendation: We recommend that Department management establish policies and procedures to monitor the Supervisors' handling of voter registration records maintenance, including the correction of registration records when warranted. We also recommend that Department management:

- Strengthen voter registration records maintenance activity controls to better account for non-demographic voter record changes.
- Appropriately identify all potential duplicate, deceased, and convicted felon voter registration records.
- Take appropriate action to promote the integrity of the State's voter registration records.

Department Response: The Department has a primary role in identifying certain voter registration records to be reviewed by Supervisors of Elections for accuracy and voter eligibility. List maintenance refers to activities conducted at the state and/or local level to protect the integrity of the electoral process by ensuring the maintenance of those records in the statewide voter registration system. The activities include but are not limited to duplicate registrations, deceased voters, those adjudicated mentally incapacitated with respect to voting and who have not had their voting rights restored, and those who have been convicted of a felony conviction and have not had their voting rights restored. However, Supervisors of Elections have sole authority to make the final determination of action taken on a voter record including changing or correcting voter records, or adding or removing registered voters from the rolls.

Since 2006 when the Florida Voter Registration System was first implemented, the Department has developed procedures to identify voter registration records that need to be reviewed for ineligibility or quality assurance or control. Current established match criteria have been refined over time based on availability of data sources, feedback from Supervisors of Elections and enhanced interagency and internal automated and manual processes. The match criteria were developed to ensure credible and reliable matches and errs on the side of the voter.

Duplicate Registrations

To identify more than one voter record in the Florida Voter Registration System that might have been created for the same voter, the Department uses the match criteria of at least three demographics before forwarding a potentially ineligible voter to Supervisors of Elections. The duplicate matches are made as long as both records fall into the above listed match criteria. Any demographic data changes to an existing voter record will allow for a duplicate check to be utilized and match identified if a duplicate record is found. The Department will continue to review and analyze existing match criteria to ascertain whether changes may be needed to strengthen and enhance the process, while still minimizing false positives. The Department will be looking further into all non-demographic data changes on existing voter records to see if that will allow an enhancement for additional duplicate voter checks. As noted above, refining of the match process has occurred over a number of years, but the Department continually looks for ways to improve the match process and will utilize the records identified by the auditors in the course of such review and analysis.

The Department will continue to identify ways to enhance the follow up procedures with the Supervisors of Elections, including additional review of invalidations and soliciting reasons for same in some instances. The Department will continue to strengthen voter registration records maintenance activity system controls so as to trigger automatic review of non-demographic record changes, which may increase the opportunities for review of potentially duplicate records as notated above.

Deceased Voters

To identify potentially deceased voters, the Department uses deceased records from the Social Security Administration and the Bureau of Vital Statistics based on established match criteria. With the exception of those few exact data matches on all criteria that are automatically forwarded to the Supervisors of Elections, the remaining potential deceased matches are manually reviewed using at least (3) demographic criteria. This secondary level review ensures the credibility and reliability of the deceased matches and protects against removal of eligible voters. As with other potentially ineligible voters, only Supervisors of Elections can remove voters from the voter rolls, so all potential matches are forwarded to Supervisors for review and removal, if appropriate.

Similar to duplicate matches, above, the Department will continue to review and analyze existing match criteria for deceased records to ascertain whether changes may be needed to strengthen the process and ensure matches are not missed due to such things as a name misspelling, incorrectly recorded date of birth, or other closely aligned demographic information. Also similar to the duplicate registration process, the Department will continue to identify ways to enhance the follow up procedures with the Supervisors of Elections, including additional review of invalidations and soliciting reasons for same in some instances. The Department notes that currently it periodically automates re-review of invalidated deceased matches and will re-send a match to the county in some instances, and will continue to enhance the follow-up process.

Lastly, the Department will work with the auditors to analyze the records and circumstances of the voters whom the auditors believe to have been deceased when ballots were cast in their names, and ensure that such information, if established, is forwarded to prosecuting authorities in the appropriate jurisdictions.

Felon Records

As it relates to felon matches, the Department uses two distinct criteria in the felon matching process: one for the automated match and the other for processing/reviewing the automated match. The Auditor General utilized a different set of match criteria. The automated match process utilizes the Florida Department of Law Enforcement (FDLE) and the Florida Department of Corrections (DOC) databases for potential matches. After the automated match process identifies a potentially ineligible voter on the basis of a prior or new felony, Department staff conduct a thorough and individualized review of all relevant records to assess whether the voter has had voting rights restored, or has completed all terms of the criminal sentence. This second step is not automated and must be done individually for each potentially ineligible voter. The fact that an active voter has a prior felony conviction does not, standing alone, mean the voter was ineligible to vote.

The Department continues to work in partnership with Supervisors of Elections to enhance integrity of records, with recent additional emphasis and encouragement to Supervisors to take statutorily authorized and directed independent action upon direct receipt of ineligibility information such as real-time conviction records from Clerks of Courts. This allows for a more immediate review than a match coming first to the Department through DOC or FDLE, is authorized and directed by Florida law, and further increases the likelihood that an appropriate match will be caught and acted upon promptly. Recent data from Clerks of Court allows for more efficient review and decision making and enhances the accuracy and integrity of records

Conclusion

Under the existing statutory scheme, the Department of State identifies potentially ineligible voters at the state level for resolution at the local level. Supervisors of Elections are not precluded from identifying potentially ineligible registered voters or conducting their own quality control checks for voter records within their counties. However, Supervisors of Elections have sole authority to determine a voter's ineligibility and to remove a voter from the voter roll.

In fulfilling its duties, the Department has established procedures and controls in place, including during the specified audit period, that regularly identify at the state level records that Supervisors of Elections must examine and address, as appropriate. In addition to continuous review of voter registration data and list maintenance activities at the state level, the Department provides a number of records maintenance reports to the Supervisors of Elections. For example, the Department makes available "Aged Reports" to the Supervisors to remind them that action is overdue on state identified potential ineligible files within their county. The "Aged Reports" mentioned in this section pertain to matches that have been sent to the Supervisor of Election offices that are still pending and have not been acted on for a final determination (Example: Felon

pending greater than 120 days, Deceased pending greater than 7 days, and any outstanding Duplicate matches. The Department also periodically identifies for county review all voter records with dates of birth exceeding 115 years of age as the record may be presumptively a deceased voter or a record with a data operator input error.

Additionally, as a result of joining the Electronic Registration Information Center (ERIC), a multi-state information sharing database, in 2019, Florida has tapped into an additional data source and invaluable tool to ensure the integrity of the voter rolls. to identify duplicate records and deceased voters, along with voters who are registered in multiple states. Florida has already completed Phase I of its implementation to incorporate in-state and deceased reports into its existing processes and is regularly making this information available to the Supervisors of Elections. Phase II of implementation will include additional reports including address changes and interstate duplicate records.

The Department's matching criteria and procedures reflect years of working internally and with the Supervisors of Elections. These established criteria and procedures seek to minimize the number of false positive matches and the risk of removing an otherwise eligible registered voter. The Department continually strives, through both intrinsic internal efforts and applying external critique and feedback such as the audit at issue, to modernize and enhance both its automated and manual processes to identify records of voters who may be ineligible and to conduct quality list maintenance activities that ensure the integrity of the voter rolls.

Finding 2: Registration Records Accuracy

Department controls for ensuring that persons who register or preregister to vote satisfy statutory age requirements and for analyzing the reasonableness of the recorded dates of birth for voters need improvement.

Recommendation: To ensure the accuracy of voter registration records and that such records support the eligibility of persons registered or pre-registered to vote in accordance with State law, we recommend that Department management strengthen age-based logical data analysis procedures and work with the Supervisors to address issues, if any, identified by the procedures.

Department Response: The Department has controls in place to prevent a person who is underage to register as an active voter, instead they are placed in a pre-registered status. The Department will work with Supervisors of Elections and their county's local voter registration system support vendor to develop a process to restore a registration record to pre-registration status if the date of birth data entry error results in an underage active registered voter.

Finding 3: Voter Address List and Registration Records Maintenance Certifications

Department records did not always evidence the timely receipt of forms from county Supervisors of Elections certifying that voter address and voter registration records maintenance activities were conducted in accordance with State law nor evidence Department review of such forms.

Recommendation: We recommend that Department management enhance controls to ensure that adequate documentation evidencing the timely receipt and review of Address List and Registration Records forms from all Supervisors is maintained in Department records.

Department Response: The Department has implemented enhanced mechanisms for recording the receipt and review of the list maintenance reports to also include the date, time, and method of receipt.

Finding 4: IT Access Privilege Controls

Department information technology (IT) access privilege controls for the Voter Focus application, the Bureau of Voter Registration Services Application, and the Department network need enhancement.

Recommendation: We recommend that Department management strengthen IT policies and procedures to ensure that:

- Periodic reviews of user access privileges are conducted and documented.
- User access privileges are timely disabled upon a user's separation from Department employment or when access is no longer needed.
- User access privileges are limited to promote an appropriate separation of duties.

Department Response: The Department will work to strengthen IT policies and procedures to ensure periodic reviews of user access privileges are conducted and documented, user access privileges are timely disabled upon a user's separation from Department employment or when access is no longer needed, and user access privileges are limited to promote an appropriate separation of duties.

Finding 5: Configuration Management Controls

Department configuration management controls need improvement to ensure that Department records evidence the authorization, review, testing, and approval of IT system changes.

Recommendation: We recommend that Department management strengthen IT policies and procedures to ensure that Department records evidence the entire configuration management process for each system change.

Department Response: Over the two-year course of this audit, the Department has made changes to strengthen IT policies and procedures to ensure that Department records evidence the entire configuration management process for each system change.

Finding 6: Records Retention

Contrary to the State of Florida *General Records Schedule GS1-SL for State and Local Government Agencies* retention requirements, the Department did not retain access control records related to the disablement of network access privileges.

Recommendation: We recommend that Department management ensure that network access control records are retained in accordance with the General Records Schedule.

Department Response: The Department retains Control Access forms for over one year. The Department has ensured that network access control records will be retained in accordance with the *General Records Schedule GS1-SL for State and Local Government Agencies*.

Finding 7: Security Controls – User Authentication

Certain security controls related to network user authentication need improvement to ensure the confidentiality, integrity, and availability of Department data and IT resources.

Recommendation: We recommend that Department management improve certain security controls related to network user authentication to ensure the confidentiality, integrity, and availability of Department data and related IT resources.

Department Response: The Department has taken measures to improve the security controls related to network user authentication to ensure the confidentiality, integrity, and availability of Department data and related IT resources.

Finding 8: HAVA Grant Administration

The Department did not adequately evaluate the Supervisors of Elections' risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the subawards associated with the 2018 Help America Vote Act Election Security Grants. Additionally, the Department did not correctly identify certain Federal award information to the Supervisors of Elections in the subaward agreements.

Recommendation: We recommend that Department management enhance controls to ensure that all Federal awards are administered in accordance with applicable Federal requirements, including those requiring an evaluation of subrecipient risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the

subaward and correct identification of Federal award information in subaward agreements.

Department Response: The Department will work to implement procedures to enhance controls to ensure that all Federal awards are administered in accordance with applicable Federal requirements, to include those requiring an evaluation of sub-recipient risk. More specifically, the Department will be implementing procedures at the start of each grant award program to complete a risk assessment. Any county that is ranked at a high risk level will be monitored and a post-award audit conducted after the final expenditure report is submitted. Random post-award audits will be completed of any county that is ranked at a medium risk level. Additionally, the Department corrected identification of Federal award information in sub-award agreements.

Finding 9: Mobile Devices

Department controls over mobile device assignment, use, and disposal and for the retention of text messages in accordance with State law need improvement.

Recommendation: We recommend that Department management designate a mobile devices administrator responsible for the management of the Department's mobile device program. We also recommend that Department management enhance mobile device controls, including mobile device policies and procedures, to ensure that:

- Department records evidence all Department-owned mobile devices assigned to employees.
- Monthly personal usage certifications are obtained from all employees assigned a Department-owned mobile device.
- Mobile device assignments and plans are periodically reviewed by the mobile devices administrator for appropriateness and cost-effectiveness.
- Mobile devices are returned to the Department upon an employee's separation from Department employment.
- Department records evidence the sanitization of mobile devices prior to disposal.
- Any text messages are retained in accordance with State law and the State's records retention schedule.

Department Response: The Department has identified a mobile devices administrator who is responsible for the management of the Department's mobile devices. The Department has reviewed the policies and procedures currently in place and updated the procedures to ensure effective controls and management of mobile devices.

Finding 10: Mobile Device Security Controls

Security controls over mobile device utilization need improvement to ensure the confidentiality, integrity, and availability of Department data and IT resources.

Recommendation: We recommend that Department management enhance certain security controls related to employee and contractor use of mobile devices to ensure the confidentiality, integrity, and availability of Department data and IT resources.

Department Response: The Department has implemented controls which enhance certain security controls related to employee and contractor use of mobile devices to ensure the confidentiality, integrity, and availability of Department data and IT resources.

Finding 11: Florida Single Audit Act

Department controls over the administration of Florida Single Audit Act requirements need improvement.

Recommendation: We recommend that Department management enhance FSAA oversight processes to ensure that all non-State entities required to submit an FRP to the Department are accurately identified, FRPs are timely obtained and reviewed by the OIG, and identified instances of recipient noncompliance or other deficiencies are timely followed up on and resolved.

Department Response: The Department has implemented new procedures to ensure compliance with the FSAA.

Finding 12: FLAIR Access Controls

As similarly noted in our report No. 2017-195, Department controls over employee access to the Florida Accounting Information Resource Subsystem need improvement to reduce the risk of unauthorized disclosure, modification, or loss of Department data.

Recommendation: We recommend that Department management enhance controls to ensure the appropriate assignment and timely removal of FLAIR user access privileges. Such enhancements should include:

- Limiting FLAIR user access privileges to promote an appropriate separation of duties.
- Revising the Access Form to specify the IT system access privileges to be removed upon an employee's separation from Department employment.
- Removing FLAIR user access privileges immediately upon an employee's separation from Department employment.
- Periodically reviewing the appropriateness of FLAIR user access privileges.

Department Response: The Department has updated and implemented policy and procedures for FLAIR access control. The Department will monitor access quarterly and access will be removed for users upon termination or separation from the Department.

Finding 13: Purchasing Card Transactions and Reconciliations

Department controls need improvement to ensure that purchasing cards are only used for authorized transactions in accordance with State law, purchasing card transactions are timely approved, and purchasing card activity is promptly reconciled to supporting records.

Recommendation: We recommend that Department management strengthen purchasing card oversight controls to ensure that purchasing cards are only used for transactions in accordance with State law, purchasing card transactions are timely approved, and purchasing card activity is promptly reconciled to supporting records.

Department Response: The Department updated the purchasing card policies and procedures. The Department has strengthened oversight controls to ensure purchasing cards are used for the intended purpose in accordance with State law. Additionally, the Department has implemented procedures to monitor the purchasing card transactions daily to ensure timely approvals and that reconciliations are completed timely.

Finding 14: Purchasing Card Controls

The Department did not always timely cancel purchasing cards upon a cardholder's separation from Department employment. Additionally, Department controls for monitoring the reasonableness of purchasing cardholder assignments and timely conducting cardholder status reviews need improvement.

Recommendation: We recommend that Department management promptly cancel purchasing cards upon a cardholder's separation from Department employment and strengthen procedures to ensure the periodic monitoring of the continued need for purchasing card assignments. We also recommend that Department management take steps to ensure the timely completion of cardholder status reviews.

Department Response: The Department enhanced the purchasing card procedures to ensure periodic monitoring of the continued need for purchasing card assignments and timely completion of the cardholder status review. The Department has implemented a process to ensure timely cancellation of purchasing cards upon a cardholder's separation from the Department.

Finding 15: Property Management

As similarly noted in prior audit reports, most recently in our report No. 2017-195, the Department did not always timely record property acquisitions to Department property records. In addition, the Department did not timely reconcile physical inventory results to the property records, accurately record all property information in Department property records, or appropriately depreciate capital assets in accordance with Department of Financial Services guidance.

Recommendation: We recommend that Department management strengthen controls to ensure that Department property records are timely and accurately updated for property acquisitions. We also recommend that Department management enhance property management procedures to promote the accurate recording of each property item's condition in the property records, the timely reconciliation of physical inventory results to Department property records, and the depreciation of capital assets in accordance with DFS guidance.

Department Response: The Department has updated the property policy and procedures, which addressed recording of property item's condition, reconciliation of inventory, and depreciation of capital assets in accordance with DFS guidance.

Finding 16: Surplus IT Equipment Sanitization and Disposition Documentation

The Department had not established policies and procedures for the surplus IT equipment data sanitization and disposal process, nor did Department records evidence the specific surplus IT equipment sanitized and disposed of by a vendor.

Recommendation: We recommend that Department management establish policies and procedures for the surplus IT equipment data sanitization and disposal process. We also recommend that Department management work with the vendor to ensure Department records adequately evidence the sanitization and disposition of each surplus IT equipment item.

Department Response: The Department documented policies and procedures for the surplus IT equipment data sanitization and disposal process currently in place. Additionally, the Department will work with the vendor to ensure Department records adequately evidence the sanitization and disposition of each surplus IT equipment item.

Finding 17: Collection Safeguards

Museum of Florida History and Knott House Museum controls were not always sufficient to effectively safeguard moneys collected. A similar finding related to the Museum of Florida History was noted in our report No. 2017-195.

Recommendation: We recommend that Museum management strengthen controls over Museum and Knott House collections to ensure the logging of all check and cash collections, recording of collections transfers, and the timely deposit of funds.

Department Response: The Department strengthened controls over Museum and Knott House collections by following policies and procedures currently in place.