STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2018-211
June 2018

DEPARTMENT OF FINANCIAL SERVICES

Division of State Fire Marshal and Information Technology Controls



Sherrill F. Norman, CPA
Auditor General

Chief Financial Officer

Pursuant to Article IV, Sections 4(c) and 5(a) of the State Constitution, the Chief Financial Officer is an elected member of the Cabinet and serves as the chief fiscal officer of the State. Pursuant to Section 20.121(1), Florida Statutes, the Chief Financial Officer is the head of the Department of Financial Services. The Honorable Jeff Atwater served as Chief Financial Officer during the period of our audit.

The team leader was Frank Belt, CPA, and the audit was supervised by Samantha Perry, CPA.

Please address inquiries regarding this report to Karen Van Amburg, CPA, Audit Manager, by e-mail at karenvanamburg@aud.state.fl.us or by telephone at (850) 412-2766.

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 FINANCIAL SERVICES

Division of State Fire Marshal and Information Technology Controls

SUMMARY

This operational audit of the Department of Financial Services (Department) focused on the Division of State Fire Marshal and selected information technology controls. The audit also included a follow-up on applicable findings noted in our report Nos. 2014-020 and 2016-069. Our audit disclosed the following:

Bureau of Fire Prevention

Finding 1: The Bureau of Fire Prevention could not demonstrate that all buildings subject to fire safety inspections were included in CitizenServe.[1] Additionally, CitizenServe included inaccurate and incomplete building inspection data.

Finding 2: Contrary to State law, the Bureau of Fire Prevention did not inspect certain State-owned buildings designated as high-hazard during the 2015-16 fiscal year.

Finding 3: Bureau of Fire Prevention policies and procedures did not specify the methodology for conducting and documenting inspections, communicating inspection results, or following up on noted violations. Additionally, inspections and follow-up inspection activities were not always adequately documented.

Finding 4: Bureau of Fire Prevention policies and procedures did not address the inspection and plan review fee invoicing process and the Bureau had not analyzed whether fire safety inspection and plan review fees are sufficient to recover inspection and review costs since the fees were established in 2001. In addition, the Bureau did not always invoice or calculate inspection and plan review fees in accordance with State law and Department rules.

Finding 5: The Bureau of Fire Prevention did not receive payment of inspection fees due from State universities.

Bureau of Fire Standards and Training

Finding 6: Bureau of Fire Standards and Training records did not always demonstrate that Florida State Fire College instructors met certification requirements.

Information Technology Controls

Finding 7: Certain security controls related to user authentication for CitizenServe and the Fire College Department of Insurance Continuing Education (FCDICE) System need improvement to ensure the confidentiality, integrity, and availability of Department data and related information technology resources.

Finding 8: During the period July 2015 through January 2017, the Division of State Fire Marshal did not conduct periodic reviews of CitizenServe or FCDICE System user access privileges.

[1] CitizenServe is a Web-based software application utilized by the Bureau of Fire Prevention to maintain inspection data and records, including inspection reports and documentation related to violations noted during an inspection.

Finding 9: Department records did not evidence that CitizenServe access privileges were timely deactivated upon an employee's separation from Department employment. Additionally, Department supervisors sometimes used CitizenServe user accounts after an employee separated from Department employment and the Department did not always timely deactivate user access privileges to the FCDICE System upon an employee's separation from Department employment.

Finding 10: The Department did not make or obtain an independent and periodic assessment of the effectiveness of relevant service organization controls for CitizenServe.

Finding 11: Contrary to State law, the Department's Information Security Manager did not report directly to the Chief Financial Officer.

BACKGROUND

The Department of Financial Services (Department) is responsible for a broad range of financial, regulatory, and consumer protection activities. To carry out these activities, the Department is organized into one office and 13 divisions, including the Division of State Fire Marshal (Division).[2] For the 2017-18 fiscal year, the Legislature appropriated approximately $370 million to the Department and authorized 2,607.50 positions, including 106 positions assigned to the Division.[3]

FINDINGS AND RECOMMENDATIONS

BUREAU OF FIRE PREVENTION

The Division, Bureau of Fire Prevention, is responsible for reviewing construction plans for all State-owned and State-leased buildings for compliance with the Florida Fire Prevention Code (Fire Code);[4] enforcing the Fire Code through inspections of State-owned buildings, such as State correctional institutions, State universities, and the Capitol Building; licensing fire equipment, engineered fire protection systems, and explosives and sparklers; and ensuring the safety of boilers in public buildings by administering and enforcing the Boiler Safety Act.[5]

State law[6] requires State-owned buildings designated as high-hazard[7] to be inspected at least annually and all other buildings to be inspected on a recurring basis as established by Department rules.[8] State law also requires the Division, within 7 days of each inspection, to submit an inspection report to the head of the State agency responsible for the building.

[2] Section 20.121, Florida Statutes.

[3] Chapter 2017-70, Laws of Florida.

[4] Department Rules, Chapter 69A-60, Florida Administrative Code.

[5] Chapter 554, Florida Statutes.

[6] Section 633.218(1), Florida Statutes.

[7] Section 633.218(1)(e), Florida Statutes, defines a "high-hazard occupancy" building as any structure: 1) that contains combustible or explosive matter or flammable conditions dangerous to the safety of life or property; 2) at which persons receive educational instruction; 3) at which persons reside, excluding private dwellings; or 4) containing three or more floor levels.

[8] Department Rule 69A-3.011, Florida Administrative Code, specifies that recurring basis shall mean annually if permitted by available resources, but at least once every 2 years, as determined by the Division.

The Department contracted with a service organization for the use of CitizenServe, a Web-based software application that provides the Bureau of Fire Prevention a single platform for licensing, inspection, and invoicing functions. Bureau of Fire Prevention staff utilize CitizenServe to maintain inspection data and records, including inspection reports and documentation related to violations noted during an inspection. According to CitizenServe records, the Bureau conducted 11,721 high-hazard inspections and 10,686 recurring inspections of 14,590 buildings during the 19-month period July 2015 through January 2017.

Finding 1: Building Inspection Data

To fulfill its statutory fire safety inspection responsibilities, it is essential that the Bureau of Fire Prevention maintain a current, comprehensive listing of buildings subject to inspection. State law[9] requires the Bureau to identify State-owned buildings using the United States National Grid (USNG) standard.[10] Bureau staff maintained all State-owned building inspection data in CitizenServe, which includes various fields to identify buildings, such as the building's location (USNG coordinates, address, and county) and applicable State agency. CitizenServe also includes fields indicating the building type (e.g., high-hazard, construction), status (active or inactive), and disposition (whether the building was occupied, unoccupied, or demolished). Bureau management and inspectors used these fields to determine the need and frequency for a fire safety inspection. As of March 14, 2017, CitizenServe included records for 26,172 State-owned buildings.

As part of our audit, we evaluated Bureau of Fire Prevention controls for ensuring all buildings subject to inspection were included in CitizenServe. Our audit procedures disclosed that Bureau management could not demonstrate that all buildings subject to inspection were included in CitizenServe. Specifically, the Bureau did not perform procedures to verify the completeness of CitizenServe building records. Such procedures could include periodic comparisons of building information included in CitizenServe to information included in other property databases such as the Florida State-Owned Lands and Records Information System (FL-SOLARIS)[11] or the Department's Origami Risk Insurance Management System (Origami).[12]

We also performed inquiries of Bureau of Fire Prevention management and evaluated Bureau policies and procedures and noted that the policies and procedures did not address requirements for documenting building and inspection data in CitizenServe. Additionally, we examined CitizenServe records as of March 14, 2017, and noted that the Bureau did not maintain building USNG coordinates in CitizenServe, data fields were sometimes blank, and the information reported was not always accurate. Specifically, we noted that:

- The USNG coordinates were not recorded for the 26,172 State-owned buildings listed in CitizenServe.

[9] Section 633.218(1)(f), Florida Statutes.

[10] The Federal Geographic Data Committee's USNG standard provides a grid reference system that is seamless across jurisdictional boundaries.

[11] FL-SOLARIS is a comprehensive database of all real property owned, lease, rented, or otherwise occupied by a State government entity and is maintained by the Department of Environmental Protection and Department of Management Services.

[12] Origami is the Department's insurance management system that includes insured property data.

- The building type field for 527 buildings was blank.
- The State agency field for 233 buildings was blank.
- The county field for 90 buildings was blank.
- The address field for 90 buildings was blank or marked unknown.
- 328 buildings were designated as construction building type. Our review of CitizenServe building data for 10 of the buildings disclosed that 9 of the buildings should have been designated as inactive.

We also examined CitizenServe records for 56 buildings designated as high-hazard. Our examination disclosed that:

- The building status for 9 buildings was not accurate.
- The building disposition for 42 buildings was blank.

In response to our audit inquiry, Bureau of Fire Prevention management indicated that workload issues precluded the input of USNG coordinates in CitizenServe. In addition, Bureau management indicated that the absence of consistent building information between CitizenServe and other systems such as FL-SOLARIS or Origami makes comparisons of the information labor-intensive. Bureau management also indicated that issues related to the transition to CitizenServe had precluded the Bureau from establishing policies and procedures addressing requirements for documenting building and inspection data.

Absent complete and accurate CitizenServe data, Bureau of Fire Prevention management's ability to effectively manage building fire safety inspections and ensure that buildings are inspected in accordance with State law and Department rules is reduced.

Recommendation: We recommend that Bureau of Fire Prevention management perform procedures to verify the completeness of CitizenServe data and input into CitizenServe the USNG coordinates for all buildings subject to inspection. We also recommend that Bureau management enhance policies and procedures for documenting building inspection data in CitizenServe and periodically review the accuracy and completeness of CitizenServe data.

Finding 2: Inspections of High-Hazard Buildings

As previously noted, State law[13] requires State-owned buildings designated as high-hazard to be inspected at least annually. As part of our audit, we requested and Department management provided, a listing from CitizenServe of inspections conducted during the 2014-15 and 2015-16 fiscal years. Our examination of the listing identified 21 State-owned buildings designated as high-hazard that the Bureau of Fire Prevention inspected during the 2014-15 fiscal year, but did not inspect during the 2015-16 fiscal year. The buildings not inspected included, for example, a State university health science center, a State agency central plant, and a State correctional institution multi-purpose building.

In response to our audit inquiry, Bureau of Fire Prevention management indicated that the inspections were not conducted due to staff oversight and turnover. Bureau management also indicated that they had not established procedures to identify instances where inspections were not completed. Fire safety

[13] Section 633.218(1), Florida Statutes.

inspections of high-hazard buildings on at least an annual basis provide greater assurance that such buildings comply with the Fire Code and help to minimize the potential loss of life and property due to the risk of fire.

Recommendation: We recommend that Bureau of Fire Prevention management establish procedures to ensure that all high-hazard buildings are inspected annually as required by State law. Such procedures should include efforts to identify any high-hazard buildings that were not timely inspected.

Finding 3: Inspection Documentation

Bureau of Fire Prevention policies and procedures[14] specified that, while conducting an inspection, inspectors were to identify fire hazards outside and inside the building; detect potential fire causes; consider potential avenues for the spread of fire; ensure life safety features were not compromised; and ensure that installed fire detection, alarm, and extinguishing systems were in a state of readiness. An inspection checklist, which listed inspection areas such as fire suppression systems, fire alarm systems, means of egress, and fire drills completed, was available in CitizenServe for inspectors to complete. Inspectors were to note any deficiencies in CitizenServe and complete an inspection report in CitizenServe. Upon conclusion of the inspection, the inspector was to conduct a closing interview with the Building Manager and notify the Building Manager of all violations noted in the inspection report. Department rules[15] require that fire safety violations be resolved within a reasonable period of time after inspection.[16]

According to Department records, the Bureau of Fire Prevention completed 22,407 inspections of 14,590 State-owned buildings during the period July 2015 through January 2017. As part of our audit and evaluation of Bureau inspection activities, we interviewed Bureau management, reviewed Bureau policies and procedures, and examined records for 59 inspections (conducted of 40 State-owned buildings) with recorded inspection dates during the period July 2015 through January 2017. Our audit procedures disclosed that:

- Although Bureau policies and procedures included general inspection guidance, the policies and procedures did not detail the methodology to be used to conduct inspections or specify how inspection activities should be documented.
- For 12 inspections, although CitizenServe records indicated that the building had a life safety system, the inspection records did not evidence that the Bureau verified that the system had been inspected by a qualified outside contractor. State law[17] requires that life safety systems, including fire suppression equipment, fire protection systems, and fire alarm system equipment, be inspected in accordance with applicable standards of the National Fire Protection Association. In response to our audit inquiry, Bureau management indicated that Bureau inspectors are not required to retain copies of life safety system inspection records.

[14] Bureau of Fire Prevention Quality Management System Procedure 3.03 I, *Annual Life Safety Inspection Procedures*.

[15] Department Rule 69A-3.012(3), Florida Administrative Code.

[16] Department Rule 69A-3.012(3), Florida Administrative Code, defines within a reasonable period of time as the amount of time it would normally take to correct a specific fire code violation, under the assumption that the property owner would begin to correct the violations upon receipt of an official document from the enforcing agency.

[17] Sections 633.306, 633.334, and 633.348, Florida Statutes.

- For 20 inspections, while the inspectors completed an inspection report, the inspectors did not complete an inspection checklist or otherwise document the actions completed during the 20 inspections. In response to our audit inquiry, Bureau management indicated that inspectors were not required to complete an inspection checklist.
- Inspection reports for 3 inspections were not included in CitizenServe due to inspector oversight.
- For all 59 inspections, no documentation was available evidencing that a closing interview was conducted with the Building Manager. In addition, for 47 inspections, no documentation was available evidencing that the inspection report was submitted to the head of the State agency responsible for the building. In response to our audit inquiry, Bureau management indicated that Bureau policies and procedures did not require inspectors to document the closing interview or submittal of the inspection report to the head of the applicable State agency.
- The inspector noted fire safety violations in the reports for 11 inspections. Our examination of CitizenServe records disclosed that, as of August 2017, the violations noted during 9 of the inspections had not been closed and 248 to 661 days (an average of 492 days) had elapsed since the violations were noted. While CitizenServe records indicated that the violations noted during the other 2 inspections had been closed, Bureau records did not evidence the basis for the inspector's conclusion that the violations had been corrected. In response to our audit inquiry, Bureau management indicated that Bureau policies and procedures do not require inspectors to document the inspector's actions to verify the correction of violations.

Absent adequate documentation demonstrating the inspection activities performed, the communication of inspection results to building managers and applicable State agency heads, and the follow-up actions taken to resolve noted violations, the Bureau of Fire Prevention cannot demonstrate that inspections are conducted in accordance with State law, Department rules, and Bureau policies and procedures.

Recommendation: We recommend that Bureau of Fire Prevention management enhance Bureau policies and procedures to specify the methodology for conducting and documenting inspection activities, communicating inspection results, and following up on noted violations. We also recommend that Bureau management ensure that inspections and follow-up inspection activities are appropriately documented in CitizenServe.

Finding 4: Inspection and Plan Review Fees

State law[18] and Department rules[19] require the Division to adopt a schedule of fees that will recover the costs of inspections; fire safety reviews of plans for proposed construction, renovations, or changes in occupancy; and the related administrative expenses. Department rules[20] specify that the fees are to be based on the value of the space, with a $100 minimum fee for each building inspection or plan review. Additional inspections required because of code violations found during the final plan review inspection are to be billed at a rate of $65 per hour, per inspector, plus expenses. Additionally, Department rules require State agencies to pay plan review fees before the review process begins. According to Department records, the Department received inspection and plan review fee revenues totaling approximately $1.5 million during the 2015-16 fiscal year.

[18] Section 633.218(5), Florida Statutes.

[19] Department Rule 69A-52.002, Florida Administrative Code.

[20] Department Rule 69A-52.004, Florida Administrative Code.

As part of our audit, we inquired of Bureau of Fire Prevention management to determine whether the Bureau had established sufficient controls, including policies and procedures, for ensuring that fire safety inspection and plan review fees were billed and collected in accordance with State law and Department rules. Our audit inquiries disclosed that the Bureau had not established policies and procedures for the fee invoicing process and that the Bureau had not analyzed, since fire safety inspection and plan review fees were established in 2001, whether the fees charged were sufficient to recover the inspection and review costs. In addition, Bureau management indicated that the Bureau had never billed State entities the $65 per hour, per inspector, fee for additional inspections required as a result of code violations found during the final plan review inspections and the amount of foregone fees cannot be determined.

We also analyzed Bureau of Fire Prevention records related to the calculation and invoicing of State entity annual inspection and plan review fees for the 2015-16 fiscal year. Our audit procedures disclosed that the Bureau did not always invoice or calculate inspection and plan review fees in accordance with Department rules. Specifically:

- Contrary to Department rules, the Bureau did not collect plan review fees from State entities prior to commencing plan reviews. In response to our audit inquiry, Bureau management indicated that State entities were not invoiced prior to starting plan reviews to avoid delays in construction projects.
- The Bureau did not assess inspection fees based on the value of each building inspected or bill State entities the $100 minimum fee when the fee for a building inspection would have been less than $100. Instead, the Bureau calculated each State entity's fees based on the total insured value of the State entity's buildings. In response to our audit inquiry, Bureau management indicated that staffing limitations prevented a detailed calculation of each building's fees.

Effective controls for the fee invoicing process, including written policies and procedures, are necessary to ensure that the Bureau of Fire Prevention calculates and bills inspection fees in accordance with Department rules. In addition, absent a current analysis of fire safety inspection and plan review fees and related costs, Bureau management cannot adequately demonstrate that fees are established at an appropriate cost-recovery level as required by State law.

Recommendation: We recommend that Bureau of Fire Prevention management establish policies and procedures addressing the inspection and plan review fee invoicing process. We also recommend that Bureau management calculate and collect inspection and plan review fees in accordance with State law and Department rules.

Finding 5: Payment of Inspection Fees

State law[21] requires each State entity to request in its annual budget proposal sufficient funds to correct any fire safety deficiencies noted by the Division and to pay for any charges or fees imposed by the Division for reviewing building or renovation plans, occupancy changes, or inspections. According to Department rules,[22] the Division is to bill State entities for annual fire inspection fees by September 1st for all space owned by the entity. Department rules also allow for the fees to be paid in equal quarterly installments, with the final payment due June 1st.

[21] Section 633.218(1)(c) and (d), Florida Statutes.

[22] Department Rule 69A-52.004(2)(b)1., Florida Administrative Code.

As part of our audit, we examined Division billing records for the 2015-16 fiscal year and noted that the Division had not received payment for inspection fees due from the State's 12 universities. According to Division records, as of June 2017, the State universities owed inspection fees totaling $4,591,899 for the Division's 2014-15 and 2015-16 fiscal year inspection activities. In response to our audit inquiry, Division management indicated that, prior to the 2015-16 fiscal year, the Division had not billed the State universities since at least the 2008-09 fiscal year. While the State University System Board of Governors 2017-18 legislative budget request included $2,271,648 to pay inspection fees for 2016-17 fiscal year inspection activities, the funds were not appropriated by the Legislature.

Payment of inspection fees owed by all State entities would better ensure that Division fee revenue is sufficient to cover Division inspection costs.

Recommendation: We recommend that Division management continue to quantify the inspection fees due from the State universities so that the State University System Board of Governors can request the applicable amount of funding.

BUREAU OF FIRE STANDARDS AND TRAINING

The Division, Bureau of Fire Standards and Training, is responsible for approving firefighter training curricula, offering training at the Florida State Fire College (Fire College), and certifying that fire service members meet industry-based standards. As of March 2018, the Fire College employed 2 full-time instructors and 34 part-time instructors. During the 2016-17 fiscal year, Bureau expenditures totaled approximately $3.2 million.

Finding 6: Fire College Instructor Certification

Department rules[23] establish minimum certification requirements for instructors who conduct training and education classes for fire service personnel. To become a certified instructor, individuals must:

- Submit an application to the Bureau of Fire Standards and Training;
- Complete specified fire services courses;
- Pass the applicable State examination; and
- Demonstrate compliance with other certification requirements, for example, 6 years of experience as a member of an organized fire department.

The Bureau utilizes the Web-based Fire College Department of Insurance Continuing Education (FCDICE) System to maintain Fire College course and instructor information. During the period July 2015 through January 2017, the Fire College utilized 44 instructors.

As part of our audit, we examined Bureau of Fire Standards and Training records for 15 of the 44 Fire College instructors and noted, as shown in Table 1, that Bureau records did not always evidence that instructors met all certification requirements.

[23] Department Rule 69A-37.059, Florida Administrative Code.

Table 1
Fire College Instructor Certification Documentation Deficiencies

Requirement	Number of Applicable Instructors	Number of Instructor Files with Deficiencies
Completed Application	15	4
6 Years of Experience as a Member of an Organized Fire Department	15	3
High School Diploma	3	3
Bachelor's Degree	11	4
Completion of Fire Service Course Delivery Class	15	4
Completion of Fire Service Course Design Class	12	2

Source: Department records.

In response to our audit inquiry, Bureau of Fire Standards and Training management indicated that the supporting records were not scanned into the FCDICE System and had been accidentally destroyed.

Absent documentation evidencing that instructors met all the certification requirements, the Bureau cannot demonstrate that Fire College instructors responsible for conducting training and education classes for fire service personnel are appropriately qualified.

Recommendation: We recommend that Bureau of Fire Standards and Training management ensure that Bureau records evidence that all Fire College instructors met the certification requirements specified in Department rules.

INFORMATION TECHNOLOGY CONTROLS

State law[24] 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) rules[25] establish 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 CitizenServe, FCDICE System, and other Department IT controls. As discussed in Findings 7 through 11, we noted areas in which IT controls need improvement.

Finding 7: CitizenServe and FCDICE System Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed certain security controls related to user authentication for CitizenServe and the FCDICE System 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 CitizenServe and FCDICE System user authentication, the risk is

[24] Section 282.318(4), Florida Statutes.

[25] AST Rules, Chapter 74-2, Florida Administrative Code, effective March 2016, and Agency for Enterprise Information Technology (AEIT) Rules, Chapters 71A-1 and 71A-2, Florida Administrative Code.

increased that the confidentiality, integrity, and availability of Department data and related IT resources may be compromised.

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

Finding 8: Periodic Review of Access Privileges

AST rules[26] require State agencies to periodically review user access privileges based on system categorization or assessed risk. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate. Department policies and procedures[27] required that application access privilege reviews be conducted by access control administrators at least quarterly and documentation of the reviews be maintained.

Our audit procedures disclosed that, during the period July 2015 through January 2017, Division access control administrators did not conduct periodic reviews of CitizenServe or FCDICE System user access privileges. In response to our audit inquiry, Division management indicated that reviews had not been conducted because a formal process for reviewing the appropriateness of access privileges and documenting the results had not been established.

Conducting periodic reviews of CitizenServe and FCDICE System user access privileges would increase management's assurance that assigned access privileges are authorized and remain appropriate.

Recommendation: We recommend that Division management establish a process that ensures access control administrators conduct and document periodic reviews of user access privileges to CitizenServe and the FCDICE System to verify the continued appropriateness of assigned user access privileges.

Finding 9: Access Privilege Controls

AST rules[28] require State agencies to ensure that IT access privileges are removed when access to an IT resource is no longer required. Prompt action to deactivate access privileges when an employee separates from employment or access to the IT resource is no longer required is necessary to help prevent misuse of the access privileges. Department policies and procedures[29] prohibited Department personnel from keeping user accounts open after an employee's last day of work and identified such practices as a security risk.

Our evaluation of CitizenServe and FCDICE System access privilege controls and examination of related Department records disclosed that control enhancements were needed to better demonstrate that access privileges are timely deactivated and used for only authorized purposes. Specifically, we noted that:

[26] AST Rule 74-2.003(1)(a)6., Florida Administrative Code, effective March 2016, and AEIT Rule 71A-1.007(2), Florida Administrative Code.

[27] Department Policy and Procedure 4-05, *Application Access Control Policy*.

[28] AST Rule 74-2.003(1)(a)8., Florida Administrative Code, effective March 2016, and AEIT Rule 71A-1.007(6), Florida Administrative Code.

[29] Department Policy and Procedure 4-05, *Application Access Control Policy*.

- CitizenServe does not record the date a user's access privileges are deactivated. Consequently, we were unable to evaluate whether the access privileges for CitizenServe users who separated from Department employment during the period July 2015 through January 2017 were timely deactivated.
- 3 of the 14 CitizenServe user accounts assigned to Bureau of Fire Prevention employees who separated from Department employment during the period July 2015 through January 2017 were used after the dates of employment separation. In response to our audit inquiry, Department management indicated that supervisors used the accounts to reassign buildings to other inspectors and to run reports.
- As of May 9, 2017, 1 of the 50 Department users with FCDICE System access privileges had been separated from Department employment for 172 business days.

Maintaining historical access control records would provide assurance that CitizenServe user access privileges are timely deactivated upon an employee's separation from Department employment or when access privileges are no longer required. The prompt deactivation of access privileges upon an employee's separation from Department employment and strict prohibition on the use of former employee IT resource accounts reduces the risk of unauthorized disclosure, modification, or destruction of Department data.

Recommendation: We recommend that Department management retain CitizenServe access control records sufficient to demonstrate that user access privileges are timely deactivated upon a user's separation from Department employment or when the access privileges are no longer required. We also recommend that Department management ensure that CitizenServe and FCDICE System access privileges are timely deactivated and not utilized by other Department personnel after a user separates from Department employment.

Finding 10: Service Organization Controls

The Department contracted with a service organization for CitizenServe use and support and maintenance services. As the Bureau of Fire Prevention relies on CitizenServe to execute its regulatory responsibilities, including licensing, inspection, and invoicing functions, it is incumbent upon the Department to take steps to reasonably ensure the integrity, reliability, and security of CitizenServe data. Such steps may include requiring the service organization to provide a service auditor's report[30] on the effectiveness of the controls established by the organization for CitizenServe or, alternatively, Department monitoring of the effectiveness of relevant service organization controls.

Our examination of Department contractual agreements with the CitizenServe service organization disclosed that the agreements did not include a provision requiring the service organization provide the Department a service auditor's report, nor had the Department requested or received such a report. In addition, our audit procedures disclosed that the Department had not monitored the effectiveness of relevant service organization controls. In response to our audit inquiry, Department management indicated that, prior to procuring the CitizenServe contractual agreements, the Department had not

[30] A service auditor's report, as described by the American Institute of Certified Public Accountants, Statement on Standards for Attestation Engagements No. 18, *Attestation Standards: Clarification and Recodification, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, provides information and auditor conclusions related to a service organization's controls. Service organizations make service auditors reports available to user organizations to provide assurances related to the effectiveness of the service organization's relevant internal controls.

established the Department's current standard contract template that requires service organizations to provide a service auditor's report.

Absent an evaluation of relevant service organization controls, Department management has reduced assurance that relevant internal controls supporting CitizenServe are in place and functioning effectively.

Recommendation: Because of the critical nature of CitizenServe data, we recommend that Department management make or obtain an independent and periodic assessment of the service organization's relevant internal controls.

Finding 11: Information Security Manager

State law[31] requires each State agency head to designate an information security manager (ISM) to administer the agency's IT security program.[32] State law specifies that, for information security duty purposes, the ISM report directly to the agency head. Organizational placement of the ISM outside the line of authority of those responsible for the Department's daily IT operations is essential to ensuring appropriate separation of duties between daily IT operations and the assessment and oversight of IT system security controls.

Our examination of Department records disclosed that, in October 2016, the Chief Financial Officer delegated the authority to administer the Department's IT security program to the Director of the Office of Information Technology. Additionally, the Department's ISM was organizationally located within the Office of Information Technology and reported to the Director of the Office of Information Technology, rather than directly to the Chief Financial Officer as the agency head.

Organizational placement of the ISM within the line of authority of the Director of the Office of Information Technology reduces Department management's assurances related to the objectivity and independence of the ISM function and does not comply with State law.

Recommendation: We recommend that Department management take steps to ensure that the Department ISM reports directly to the Chief Financial Officer in accordance with State law.

PRIOR AUDIT FOLLOW-UP

The Department had taken corrective actions for the applicable findings included in our report Nos. 2014-020 (finding Nos. 1 through 3) and 2016-069 (Finding 7).

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

[31] Section 282.318(4)(a), Florida Statutes.

[32] AST Rule 74-2.002(1)(f)8., Florida Administrative Code, specifies that an IT security program includes information security policies, procedures, standards, and guidelines; an information security awareness program; an information security risk management process, including a comprehensive risk assessment; a Computer Security Incident Response Team; and a disaster recovery program aligned with the agency's Continuity of Operations Plan.

information for use in promoting government accountability and stewardship and improving government operations.

We conducted this operational audit from January 2017 through August 2017 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 Financial Services (Department) focused on the Division of State Fire Marshal (Division) and selected information technology (IT) controls. 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 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 Nos. 2014-020 (finding Nos. 1 through 3) and 2016-069 (Finding 7).

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 Division operations.
- Obtained an understanding of selected Department IT controls, assessed the risks related to those controls, evaluated whether selected general and application IT controls for CitizenServe and the Fire College Department of Insurance Continuing Education (FCDICE) System were in place, and tested the effectiveness of the controls.
- Performed inquiries of Department management and examined contractual agreements between the Department and CitizenServe service organization to determine whether the Department had obtained and reviewed a service auditor's report on the effectiveness of the controls established by the organization for CitizenServe.
- Performed inquiries of Division staff and inspected selected documents and records to determine whether Division management had adequately designed and implemented controls, including policies and procedures, for conducting fire safety inspections, the efficient and effective operation of the Florida State Fire College (Fire College), and the proper acquisition, assignment, control, use, and disposition of tangible personal property.
- Analyzed CitizenServe records to determine whether the Bureau of Fire Prevention timely completed all inspections conducted during the period July 2015 through June 2016.
- From the population of 14,590 State-owned buildings that received an inspection during the period July 2015 through January 2017, examined Bureau of Fire Prevention records for 59 selected inspections completed for 40 buildings to determine whether the inspections were timely and adequately performed and documented; related inspection reports were timely provided to the responsible State agency heads; and, when applicable, follow-up activities were timely and appropriately conducted for all reported violations.
- Analyzed CitizenServe records to evaluate the appropriateness of the classification for 10 of the 10,133 State-owned buildings recorded in CitizenServe with a building type of "inactive," 5 of the 527 buildings with a recorded building type of "blank," and 10 of the 328 buildings with a recorded building type of "construction." In addition, analyzed inspection data for 30 selected buildings with a building type of "blank," including the 5 buildings analyzed for classification appropriateness, to determine whether the buildings were inspected in accordance with Section 633.218(1), Florida Statutes.
- From the population of 631 building permits requiring a construction plan review during the period July 2015 through January 2017, examined Bureau of Fire Prevention records for 10 selected building permits to determine whether the construction plan reviews were timely and adequately performed and documented; related inspection reports were timely provided to the responsible State agency heads; and, when applicable, follow-up activities were timely and appropriately conducted for all reported violations.
- Analyzed Department financial records for the 2015-16 fiscal year to determine whether fire safety inspection fee revenue was sufficient to recover related costs in accordance with State law and Department rules, and analyzed Department financial records for the period July 2015 through

January 2017 to determine whether Bureau of Fire Prevention expenditures were expended from the Insurance Regulatory Trust Fund in accordance with Section 633.132, Florida Statutes.

- Analyzed Bureau of Fire Prevention records related to the calculation of State entity annual inspection and plan review fees for the 2015-16 fiscal year to determine whether the fees were appropriately calculated.
- Examined Bureau of Fire Prevention records for 13 selected State entity annual fire safety inspection fees for the 2015-16 and 2016-17 fiscal years and 10 selected construction plan review fees for the period July 2015 through January 2017 to determine whether the fees were accurately calculated, appropriately charged, timely collected, deposited in the Insurance Regulatory Trust Fund, and appropriately recorded in the Florida Accounting Information Resource Subsystem (FLAIR).
- From the population of 15,184 State-owned buildings designated in CitizenServe as high-hazard or recurring as of March 14, 2017, selected 40 buildings with inspections during the period July 2015 through January 2017 and examined Department records for the 19 inspectors who completed the inspections to determine whether the inspectors were appropriately trained and qualified in accordance with Department rules.
- From the population of 2,914 Bureau of Fire Prevention expenditures, totaling $9,167,459, made during the period July 2015 through January 2017, examined Department records for 42 selected expenditures, totaling $85,825, to determine whether the expenditures were property supported and made in accordance with applicable laws, rules, regulations, policies and procedures, and other guidelines.
- Performed inquiries of Department and Fire College management and examined Fire College records to determine whether the Fire College developed a staffing and funding formula pursuant to Section 633.444(1)(e), Florida Statutes, and whether Fire College staffing levels were appropriate.
- From the population of 2,194 Fire College expenditures, totaling $5,768,626, made during the period July 2015 through January 2017, examined Department records for 41 selected expenditures, totaling $86,300, to determine whether the expenditures were properly supported and made in accordance with applicable laws, rules, regulations, policies and procedures, and other guidelines.
- Physically observed 40 of the 391 Fire College property items recorded in Department property records as of January 2017 to verify the existence of the items and to determine whether the information recorded in Department property records accurately reflected the physical location, serial number, and description of the items. Selected an additional 15 property items during the physical observation and determined whether the physical location, serial number, and property description for the items agreed with the information recorded in Department property records.
- Examined Department records to determine whether the Department performed a physical inventory of Fire College property during the 2015-16 fiscal year in accordance with applicable laws, Department rules, and Department policies and procedures.
- Examined Department purchasing records for the 8 Fire College property items, with acquisition costs totaling $552,305, purchased during the period July 2015 through January 2017, to determine whether the items were timely and accurately added to Department property records.
- From the population of 111 Fire College property items, with acquisition costs totaling $441,177, disposed of during the period July 2015 through January 2017, examined Department records for 22 selected property items, with acquisition costs totaling $73,187, to determine whether the property dispositions were properly documented and made in accordance with applicable laws, rules, and Department policies and procedures.

- Examined Department records as of January 31, 2017, to determine whether Department records evidenced that 15 Fire College motor vehicles, with acquisition costs totaling $293,744, were assigned and used in accordance with Department of Management Services rules and demonstrated accountability for vehicle usage.
- Analyzed Department property records as of January 2017 to determine whether Department property records included all the information required by Department rules.
- From the population of 44 Fire College instructors during the period July 2015 through January 2017, examined Department records for 15 selected instructors to determine whether the instructors met the minimum certification requirements specified in Department rules.
- Evaluated Department actions to correct finding Nos. 1 through 3 noted in our report No. 2014-020. Specifically, we:
  - Reviewed applicable laws, rules, Department policies and procedures, and other guidelines, and interviewed Department personnel to obtain an understanding of Division of Risk Management (Division) operations.
  - Performed inquiries of Division personnel and inspected selected documents and records to determine whether Division management had adequately designed and implemented controls, including policies and procedures, for:
    - Auditing claims payments, verifying and calculating the average wholesale prices for pharmaceutical benefits, and verifying the amounts paid for pharmaceutical purchases.
    - Monitoring workers' compensation program contractors.
    - Reviewing independent service auditor reports on service organization controls.
    - Reconciling financial data recorded in Origami to financial data recorded in FLAIR.
  - From the population of 3 Medical Case Management (MCM) audits and 13 Pharmacy Benefits Management (PBM) audits conducted during the period July 2015 through March 2017, examined Division records for 2 selected MCM audits and 3 selected PBM audits to determine whether the audits were performed in accordance with Division policies and procedures.
  - Inspected Division records for the six on-site monitoring visits conducted by Division personnel at three workers' compensation program providers during the period July 2015 through February 2017 to determine whether the visits were performed and monitoring reports prepared in accordance with Division policies and procedures.
  - From the population of five independent service auditor reports received by the Division during the period July 2015 through January 2017 for three service organizations, examined Division records for four selected reports to determine whether the reports adequately addressed the service organization's relevant internal controls and whether the Division timely and adequately reviewed the reports.
  - From the population of 683,152 workers' compensation claim payments, totaling $215,510,066, paid during the period July 2015 through January 2017, examined Division records for 60 selected claim payments, totaling $4,198,305, to determine whether the claims were properly filed and complete, allowable, properly recorded in Origami and FLAIR, and processed in compliance with applicable laws and regulations.
  - From the population of 46 State entities invoiced salary indemnification claims totaling $4,775,249 during the period July 2015 through January 2017, examined 3 selected monthly invoices, totaling $411,371, prepared by the Division for 4 State entities, to determine whether the claims were reimbursed by the State entity. In addition, from the population of 450 salary indemnification claim payments, totaling $411,371, examined Division records for 21 selected claims payments, totaling $13,042, to determine whether the claims were calculated correctly.

- Reviewed all *Salary Indemnification Benefits Paid to Workers' Compensation Claimants and Reimbursements by State Agencies* quarterly reports submitted by the Division to the Executive Office of the Governor and the Legislature during the period July 2015 through January 2017 to determine whether the reports were timely and appropriately submitted.
- Performed inquiries of Division personnel and inspected documents and records related to Origami edits and output controls to determine whether the Division adequately designed and implemented controls for claims payments and report preparation.
- Examined 18 selected Origami and FLAIR data reconciliations completed during the period July 2015 through January 2017 to determine whether the Division performed the reconciliations in accordance with Division policies and procedures, the duties assigned to the individuals performing the reconciliations were appropriately separated, corrective actions were taken for any reconciling items, and the reconciliations were subject to supervisory review.

- Evaluated Department actions to correct Finding 7 noted in our report No. 2016-069. Specifically, we interviewed Department personnel, reviewed Department policies and procedures, and evaluated Department compliance with statutory requirements for collecting and utilizing individuals' social security numbers.
- Reviewed applicable laws, rules, and other State guidelines to obtain an understanding of the legal framework governing Department operations.
- Observed, documented, and evaluated the effectiveness of selected Department processes and procedures for:
  - Purchasing activities.
  - The administration of tangible personal property in accordance with applicable guidelines. As of January 2017, the Department was responsible for tangible personal property with related acquisition costs totaling $53,097,659.
  - The assignment and use of motor vehicles. As of January 2017, the Department was responsible for 540 motor vehicles with related acquisition costs totaling $12,006,508.
  - The assignment and use of wireless devices with related costs totaling $1,539,792 during the period July 2015 through January 2017.
  - The administration of the requirements of the Florida Single Audit Act. During the period July 2015 through January 2017, the Department expended $1,325,512 for two 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 January 2017, the Department was responsible for 30 active 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

CHIEF FINANCIAL OFFICER
JIMMY PATRONIS
STATE OF FLORIDA

May 31, 2018

Sherrill F. Norman
Auditor General
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Pursuant to Section 11.45(4)(d), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Auditor General's operational audit of the *Division of State Fire Marshal and Information Technology Controls.*

If you have any questions concerning this response, please contact Leah Gardner, Director of Audit, at (850) 413-3112.

Sincerely,

Jimmy Patronis

JP/rlg
Enclosure

DEPARTMENT OF FINANCIAL SERVICES
THE CAPITOL, TALLAHASSEE, FLORIDA 32399-0301 • (850) 413-2850 FAX (850) 413-2950

DEPARTMENT OF FINANCIAL SERVICES' RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Building Inspection Data

The Bureau of Fire Prevention could not demonstrate that all buildings subject to fire safety inspections were included in CitizenServe. Additionally, CitizenServe included inaccurate and incomplete building inspection data.

Recommendation: We recommend that Bureau of Fire Prevention management perform procedures to verify the completeness of CitizenServe data and input into CitizenServe the USNG coordinates for all buildings subject to inspection. We also recommend that Bureau management enhance policies and procedures for documenting building inspection data in CitizenServe and periodically review the accuracy and completeness of CitizenServe data.

Response: The Bureau of Fire Prevention plans to adopt a procedure to ensure quarterly and semi-annual building inspection reviews are conducted by individual inspectors and their supervisors. As identification of USNG coordinates is subjective and requires the use of additional technology not currently available to the Division, the Bureau plans to request a statutory change removing the USNG requirement from statute. This will allow the Division the ability to explore alternate identification methods that may provide more value to the state of Florida in the identification of state-owned and state-leased buildings. Alternatively, the Division may need to explore technology available to initiate the marking and designating of all state-owned buildings by their USNG coordinates during the annual inspections of those buildings if the USNG requirement is not removed legislatively.

Expected Completion Date for Corrective Action: July 1, 2019

Finding No. 2: Inspections of High-Hazard Buildings

Contrary to State law, the Bureau of Fire Prevention did not inspect certain State-owned buildings designated as high-hazard during the 2015-16 fiscal year.

Recommendation: We recommend that Bureau of Fire Prevention management establish procedures to ensure that all high-hazard buildings are inspected annually as required by State law. Such procedures should include efforts to identify any high-hazard buildings that were not timely inspected.

Response: The Bureau of Fire Prevention plans to adopt a procedure requiring all regional supervisors review the "Building Lookup by Inspection and Region Report" on a quarterly basis to ensure every high-hazard building is inspected annually.

Expected Completion Date for Corrective Action: August 1, 2018

Finding No. 3: Inspection Documentation

Bureau of Fire Prevention policies and procedures did not specify the methodology for conducting and documenting inspections, communicating inspection results, or following up on noted violations. Additionally, inspections and follow-up inspection activities were not always adequately documented.

Recommendation: We recommend that Bureau of Fire Prevention management enhance Bureau policies and procedures to specify the methodology for conducting and documenting inspection activities, communicating inspection results, and following up on noted violations. We also recommend that Bureau management ensure that inspections and follow-up inspection activities are appropriately documented in CitizenServe.

Response: The Bureau has previously adopted an Inspection Procedures policy detailing how an inspection is to be conducted and requiring a closing interview with the Building Manager or Manager's representative. The Bureau will amend this policy to include the completion of a "Fire and Life Safety Inspection Checklist," which will be signed by the Inspector and Owner's Representative (Building Manager or Manager's representative). The Bureau has completed drafts of both documents.

Expected Completion Date for Corrective Action: July 1, 2018

Finding No. 4: Inspection and Plan Review Fees

Bureau of Fire Prevention policies and procedures did not address the inspection and plan review fee invoicing process and the Bureau had not analyzed whether fire safety inspection and plan review fees are sufficient to recover inspection and review costs since the fees were established in 2001. In addition, the Bureau did not always invoice or calculate inspection and plan review fees in accordance with State law and Department rules.

Recommendation: We recommend that Bureau of Fire Prevention management establish policies and procedures addressing the inspection and plan review fee invoicing process. We also recommend that Bureau management calculate and collect inspection and plan review fees in accordance with State law and Department rules.

Response: In fiscal years 2011-12 and 2012-13, the Department conducted regulatory reviews of all rules and business procedures, including the Bureau's fee rule. The rule and procedures were reviewed and a decision was made by Department leadership that the Bureau's revenue was sufficient to cover the Bureau's expenses, even though some individual fees were determined not to be commensurate with the services rendered.

However, the Bureau of Fire Prevention intends to seek assistance from Department leadership in conducting another analysis of inspection and plan review fees in accordance with State law and Department rules. The Bureau will also initiate rulemaking to amend its rules concerning the initiation of fees for additional inspections.

Expected Completion Date for Corrective Action: July 1, 2019

Finding No. 5: Payment of Inspection Fees

The Bureau of Fire Prevention did not receive payment of inspection fees due from State universities.

Recommendation: We recommend that Division management continue to quantify the inspection fees due from the State universities so that the State University System Board of Governors can request the applicable amount of funding.

Response: The Division intends to continue to quantify inspection fees for the State University System Board of Governors and continue to issue invoices for all inspections conducted of State universities on an annual basis, as is done for all other state agencies.

Expected Completion Date for Corrective Action: Completed

Finding No. 6: Fire College Instructor Certification

Bureau of Fire Standards and Training records did not always demonstrate that Florida State Fire College instructors met certification requirements.

Recommendation: We recommend that Bureau of Fire Standards and Training management ensure that Bureau records evidence that all Fire College instructors met the certification requirements specified in Department rules.

Response: Fire College staff has reviewed all current Instructor personnel files to ensure appropriate documentation is in place. Additional procedures have been developed and implemented to ensure future instructor files will contain appropriate documentation.

Expected Completion Date for Corrective Action: Completed

** Confidential Finding **

Finding No. 7: CitizenServe and FCDICE System Security Controls – User Authentication

Certain security controls related to user authentication for CitizenServe and the Fire College Department of Insurance Continuing Education (FCDICE) System need improvement to ensure the confidentiality, integrity, and availability of Department data and related information technology resources.

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

Response: As of January 5, 2018, the SFM implemented corrective action to partially address the user authentication concerns. The SFM will evaluate the additional authentication concerns and where appropriate, implement additional controls.

The specific controls related to this finding have been evaluated by OIT and determined to be appropriate and achievable. The development team has been provided with the detailed findings list. OIT is already planning these remediation steps and will have them implemented within one year of the date of the finding report.

Expected Completion Date for Corrective Action: May 2, 2019

Note: Due to the confidential nature of this finding, and to ensure the security of DFS systems, detailed information is not provided for this finding.

Finding No. 8: Periodic Review of Access Privileges

During the period July 2015 through January 2017, the Division of State Fire Marshal did not conduct periodic reviews of CitizenServe or FCDICE System user access privileges.

Recommendation: We recommend that Division management establish a process that ensures access control administrators conduct and document periodic reviews of user access privileges to CitizenServe and the FCDICE System to verify the continued appropriateness of assigned user access privileges.

Response: The Bureau of Fire Prevention plans to adopt a policy requiring quarterly reviews of user access privileges to CitizenServe.

Bureau of Fire Standards and Training staff is currently in the process of developing written procedures for the approval of Division leadership to approve that will serve as the basis for determining appropriate FCDICE access levels and ensuring all access levels are reviewed on an annual basis.

Expected Completion Date for Corrective Action: August 30, 2018

Finding No. 9: Access Privilege Controls

Department records did not evidence that CitizenServe access privileges were timely deactivated upon an employee's separation from Department employment. Additionally, Department supervisors sometimes used CitizenServe user accounts after an employee separated from Department employment and the Department did not always timely deactivate user access privileges to the FCDICE System upon an employee's separation from Department employment.

Recommendation: We recommend that Department management retain CitizenServe access control records sufficient to demonstrate that user access privileges are timely deactivated upon a user's separation from Department employment or when the access privileges are no longer required. We also recommend that Department management ensure that CitizenServe and FCDICE System access privileges are timely deactivated and not utilized by other Department personnel after a user separates from Department employment.

Response: The Bureau of Fire Prevention plans to adopt a policy regarding user access privileges to CitizenServe and separation of those users from the Department. Bureau of Fire Standards and Training staff is currently in the process of developing written procedures for the approval of Division leadership that will serve to consistently establish FCDICE user access when employees are hired and ensuring access privileges are removed upon employee separation.

Expected Completion Date for Corrective Action: August 30, 2018

Finding No. 10: Service Organization Controls

The Department did not make or obtain an independent and periodic assessment of the effectiveness of relevant service organization controls for CitizenServe.

Recommendation: Because of the critical nature of CitizenServe data, we recommend that Department management make or obtain an independent and periodic assessment of the service organization's relevant internal controls.

Response: This assessment was obtained during the audit. The agreement with the vendor pre-dates the current contract template that requires this assessment to be provided. Although the current contract with the vendor will not be modified, the assessment will be provided by the vendor annually. The process for making the request will be included in the State Fire Marshal's internal process documentation.

Expected Completion Date for Corrective Action: May 2, 2019

Finding No. 11: Information Security Manager

Contrary to State law, the Department's Information Security Manager did not report directly to the Chief Financial Officer.

Recommendation: We recommend that Department management take steps to ensure that the Department ISM reports directly to the Chief Financial Officer in accordance with State law.

Response: The remediation for this finding will involve a change in the organizational structure of the Department. The Department is actively working to produce the position description updates and other Human Resources administration requirements to facilitate a position change.

Expected Completion Date for Corrective Action: June 2019