STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2016-069
December 2015

DEPARTMENT OF FINANCIAL SERVICES

Division of Insurance Fraud and Selected Administrative Activities



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.

Please address inquiries regarding this report to Lisa Norman, CPA, Audit Manager, by e-mail at lisanorman@aud.state.fl.us or by telephone at (850) 412-2831.

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

www.myflorida.com/audgen

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

State of Florida Auditor General

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

DEPARTMENT OF FINANCIAL SERVICES

Division of Insurance Fraud and Selected Administrative Activities

SUMMARY

This operational audit of the Department of Financial Services (Department) focused on the Division of Insurance Fraud (Division) and selected administrative activities. Our audit also included a follow-up on the applicable findings noted in our report Nos. 2014-103 and 2015-002, and finding No. 4 noted in our report No. 2014-020. Our audit disclosed the following:

Division of Insurance Fraud

Finding 1: The Division did not always include sufficient information in the Augmented Criminal Investigative Support System (ACISS) to support the reasons referrals regarding potential insurance fraud were closed without investigation.

Finding 2: The Division did not ensure that all referrals received from the Office of Financial Regulation (OFR) were identified or accurately recorded in ACISS. In addition, contrary to the Division's Memorandum of Understanding with the OFR, the Department did not provide the OFR with information on the disposition of referrals.

Finding 3: Division investigations of potential insurance fraud were sometimes inappropriately closed in ACISS using a resource limitations reason code.

Finding 4: ACISS data processing controls need improvement to provide for the proper accounting for and processing of referrals and investigative cases.

Finding 5: ACISS controls need improvement to ensure that user access privileges are limited to only those necessary for the user's assigned job responsibilities and to demonstrate that user access privileges are timely deactivated upon an employee's separation from Department employment or when the privileges are no longer required.

Selected Administrative Activities

Finding 6: Certain security controls related to Department network authentication need improvement to better protect the confidentiality, integrity, and availability of Department data and information technology resources.

Finding 7: The Department had not established Departmentwide policies and procedures for the collection and use of social security numbers or always documented the timely evaluation of its collection and use of social security numbers to ensure compliance with State law.

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 14 divisions, including the Division of Treasury, the Division of Insurance Fraud, the Division of Consumer Services, the Division of Administration, and the Division of Information Systems.[1]

FINDINGS AND RECOMMENDATIONS

DIVISION OF INSURANCE FRAUD

State law[2] authorizes the Department to examine and investigate the affairs of every person involved in the business of insurance in the State to determine whether such persons have been or are engaged in any unfair method of competition or in any unfair or deceptive act or practice prohibited by State law. The Department, Division of Insurance Fraud (Division), is responsible for investigating suspected insurance fraud. To facilitate the conduct of investigations, the Division operated through a Headquarters office in Tallahassee, and as shown in ***EXHIBIT A*** to this report, the Division had six regional offices located throughout the State. According to Department records, Division expenditures totaled approximately $23.6 million during the 2014-15 fiscal year and, as of January 7, 2015, the Division had filled 180 of the Division's 194 authorized positions.

State law[3] specifies that Division investigators are to be certified State law enforcement officers with the authority to bear arms and make arrests for criminal violations found during investigations. Division management reported[4] that, during the 2013-14 fiscal year, Division activities resulted in 1,575 cases presented for prosecution, 1,465 arrests, 1,250 convictions, and approximately $50.5 million in court-ordered restitution payments.

The Division received referrals regarding instances of potential fraud from various sources, such as the National Insurance Crime Bureau; State agencies, including the Office of Financial Regulation; insurance companies; law enforcement agencies; and citizens. Division staff utilized the Augmented Criminal Investigative Support System (ACISS) to receive, track, and review referrals; store investigative case background information; and assign and document investigations. Referral information was electronically uploaded into ACISS through an online referral gateway or manually input into ACISS by Division staff.

As shown in Chart 1, the Division received 31,083 referrals during the period July 2013 through February 2015 and approximately 85 percent of the referrals were received from the National Insurance Crime Bureau and insurance companies. During the same period, the Division closed 29,727 of the 31,083 referrals received.

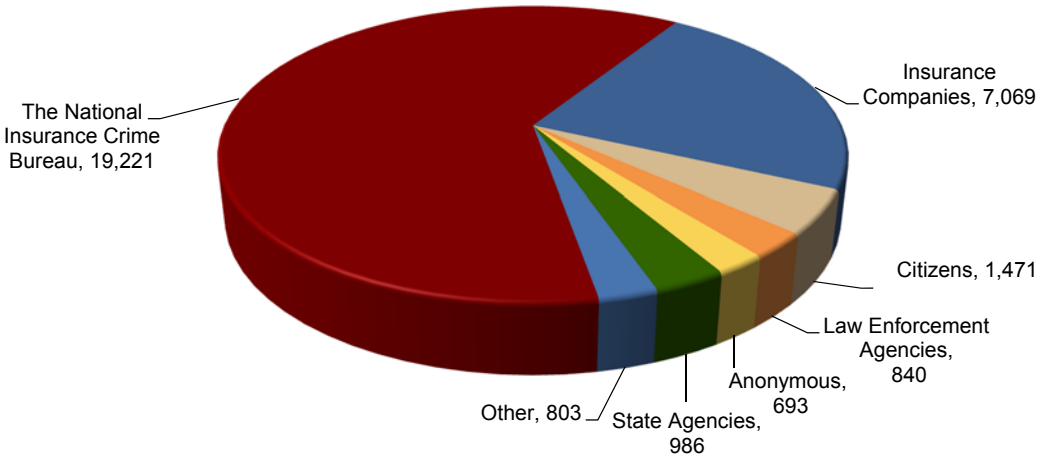
[1] Section 20.121, Florida Statutes.

[2] Section 626.9561, Florida Statutes.

[3] Section 626.989(7), Florida Statutes.

[4] Division 2013-14 *Annual Report*.

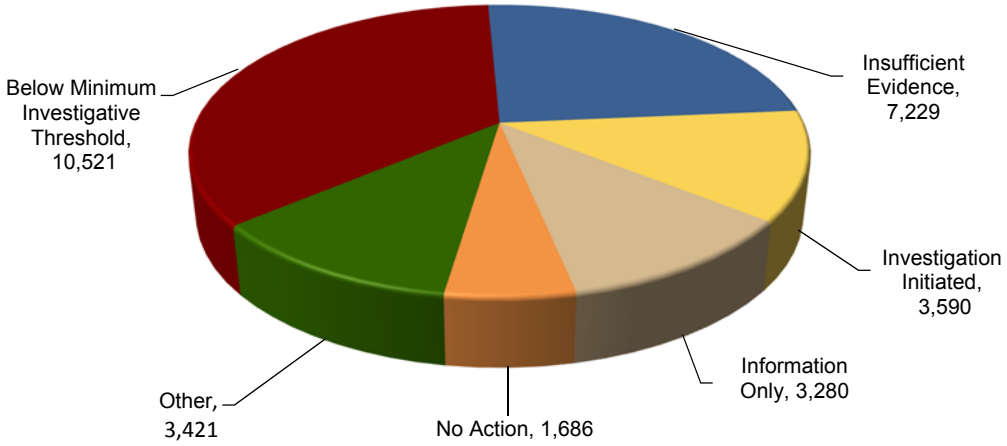
Chart 1
Sources of Referrals
During the Period July 2013 Through February 2015



Source: ACISS records as of March 31, 2015.

As shown in Chart 2, the Division indicated that, for 3,590 of the closed referrals (12 percent) investigations were initiated and that, for the remaining 26,137 closed referrals (88 percent) the referrals did not warrant investigation. One reason frequently given for a referral not warranting investigation was that there were insufficient solvability factors (below minimum investigative threshold) and another reason was insufficient evidence. As of February 28, 2015, the Division had completed 2,605 of the 3,590 investigations.

Chart 2
Reasons for Closing Referrals
During the Period July 2013 Through February 2015



Source: ACISS records as of March 31, 2015.

Finding 1: Processing of Referrals

Division regional office management were responsible for reviewing referrals and for determining whether an investigation should be initiated or closed without investigation. In deciding whether to investigate a referral, Division management was to apply various solvability factors, including, for example, the existence of witnesses, videos, audio tapes, falsified documents, and multiple claims for the same loss. Division policies and procedures[5] specified that after reviewing a referral, Division management could either forward the referral for investigation, forward the referral for further research and development, or close the referral. When closing referrals, Division policies and procedures[6] specified that Division personnel were to record the reason for closure in ACISS and were to provide the necessary documentation and explanations to support the decision to close the referrals.

Our examination of ACISS records for selected referrals received by the Division during the period July 2013 through February 2015 disclosed that the Division did not always sufficiently document the basis for closing referrals without investigation. Specifically, for 51 referrals closed in ACISS with a designated reason of *Insufficient Evidence*, *Below Minimum Investigative Threshold*,[7] or *No Action*,[8] ACISS records for 28 (55 percent) of the referrals did not include sufficient information to support the reason the referrals were closed without investigation. For example, we found that:

- For 5 referrals, Division personnel indicated in ACISS that the referrals had been closed because the referring party had not provided sufficient evidence to support the referral. We requested from Division management documentation that the investigators had communicated with the referring parties regarding the insufficient evidence. In response to our audit inquiry, Division management indicated that, for 4 of the 5 referrals, the investigators had not communicated with the referring parties. For the other referral, Division management did not indicate whether or not the investigator had communicated with the referring party and no documentation of any such communication was included in ACISS.
- For 10 referrals, Division personnel indicated in ACISS that the referrals had been closed because there were insufficient solvability factors. For another 5 referrals, Division personnel indicated that no action had been taken. For these 15 referrals, we noted that detailed explanations regarding the absence of sufficient solvability factors or why no action was necessary for these referrals had not been included in ACISS.

The inclusion of sufficient information in ACISS to document the reasons for closing referrals without investigation would better demonstrate that all referrals of potential fraud are properly considered for investigation.

Recommendation: We recommend that Division management ensure that sufficient information is included in ACISS to support decisions to close referrals without investigation.

[5] Division Policy No. 9-01, *Criminal Intelligence Analyst Unit*.

[6] Division Policy No. 8-03, *Suspected Fraud Referrals Database.*

[7] Division management defined this term to include referrals where there may have been sufficient information to support a criminal case, but there were insufficient solvability factors to pursue.

[8] Division management indicated in response to our audit inquiry that the *No Action* reason code was to be used only when a referral did not fit another category, and that use of this category required extensive written justification.

Finding 2: Office of Financial Regulation Referrals

Pursuant to a February 2013 Memorandum of Understanding (MOU) between the Office of Financial Regulation (OFR) and the Division, the OFR was to refer to the Division all cases involving suspected money service business[9] (MSB) fraud where the MSB negotiated third-party business-to-business checks totaling $500,000 or more within a 6-month period, the MSB was referred to the Department of Law Enforcement for potential felony criminal activity, or a MSB was conducting business with a person or entity identified by the Division as a known or suspected participant in an MSB-facilitated workers' compensation premium fraud scheme. The MOU also required the Division to provide the OFR with a quarterly report on the status or disposition of OFR referrals. In addition to the MOU, OFR referral letters to the Division requested the Division to provide the OFR with the disposition for referrals no later than 30 days from the date of the referral.

The Division reported in ACISS that 47 referrals were received from the OFR during the period July 2013 through February 2015. As part of our audit, we obtained from the OFR a listing of referrals submitted to the Division during the same time period and compared the listing to the referrals reported by the Division in ACISS as being received from the OFR. Our comparison disclosed that Division controls did not ensure the complete and accurate identification of OFR referrals in ACISS as our comparison identified 56 referrals made by the OFR to the Division during the period July 2013 through February 2015. Specifically, our comparison identified:

- 9 referrals from the OFR that the Division had not entered into ACISS.
- 12 referrals that were entered into ACISS, but were not coded as being received from the OFR.
- 11 referrals that had been improperly coded in ACISS as being received from the OFR.
- Other issues related to the listing of referrals from OFR.

In response to our audit inquiry, Division management indicated in July 2015 that the Division had implemented a new protocol for receipt and notification of OFR referrals, including the designation of an analyst to receive, input, and track all fraud referrals received from the OFR.

Additionally, our audit procedures disclosed that for 53 of the 56 referrals received from the OFR, Division management was unable to provide documentation demonstrating that the Division had communicated the disposition of the referrals to the OFR. Also, Division management indicated, in response to our audit inquiry, that during the period July 2013 through July 2015, the Division had not provided the OFR with quarterly reports on the status and disposition of referrals, as specified by the terms of the MOU. Division management noted that management turnover had contributed to the reporting deficiencies. Division management also indicated that a protocol had been implemented to ensure that future referral dispositions were timely communicated to the OFR in accordance with the MOU.

The complete and accurate identification of all referrals received from the OFR would better ensure that the Division appropriately considers all referrals for investigation. In addition, proper tracking of referrals

[9] Section 560.103(22), Florida Statutes, defines a money service business as any person located in or doing business in the State, from the State, or into the State from locations outside of the State or United States who acts as a payment instrument seller, foreign currency exchanger, check casher, or money transmitter.

and reporting of Division activities would better ensure that the Division provides the OFR the information specified by the MOU.

Recommendation: We recommend that Division management ensure that all referrals received from the OFR are accurately identified in ACISS and that referral disposition information is timely reported to the OFR as specified by the MOU.

Finding 3: Reasons for Closing Investigations

Investigators within the Division's regional offices were responsible for investigating suspected insurance fraud cases. Fraud investigation cases were to remain open in ACISS until the investigation was either completed or terminated for reasons such as conviction, insufficient evidence, or the allegation was unfounded. For investigations closed prior to completion, Division investigators were responsible for recording in ACISS the reason for case closure by selecting from a list of established reason codes.

According to ACISS records, Division investigators closed 3,795 investigations during the period July 2013 through February 2015. Our review of ACISS information for these investigations disclosed that, for 83 investigations involving allegations such as staged accidents, fictitious claims, and public adjuster licensee fraud, Division investigators had closed the investigations and recorded the reason code as *Closed – Due to Resource Limitations*. While we noted that, for referrals, Division management had removed from ACISS the option to select *Closed – Due to Resource Limitations* and had instructed Division staff that referrals should not be closed with this reason code, similar actions had not been taken to preclude the use of the reason code for Division investigations.

The indication of resource limitations as a reason for terminating an investigation and closing a case limits Division management's ability to demonstrate that each investigation was given adequate consideration and that appropriate conclusions and dispositions were made.

Recommendation: We recommend that Division management remove *Closed – Due to Resource Limitations* as a reason code in ACISS for closing investigations. We also recommend that Division management evaluate whether any of the investigations closed using the *Closed – Due to Resource Limitations* reason code should be reopened.

Finding 4: ACISS Data Processing Controls

Effective data processing controls are necessary to provide reasonable assurance that all transactions that occur are input into the system, accepted for processing, processed once and only once by the system, and properly included in system output. Such controls should include tools and procedures to identify, report, and correct any errors that occur during the data entry process. For example, established controls should include: 1) user error logs to provide timely follow-up and correction of unresolved data errors and irregularities, 2) an established monitoring process to assure the effectiveness of error-handling procedures, and 3) procedures to periodically review user error logs to determine the significance and nature of the data errors as well as the status of any uncorrected data errors.

ACISS automatically assigned a unique sequential number to each referral electronically received or manually input, and a unique sequential number to each investigative case established. As part of our audit, we analyzed ACISS data for the 31,083 referrals the Division received and the 3,590 investigative

cases the Division initiated during the period July 2013 through February 2015. Our analysis disclosed 618 gaps in the sequential numbering of referrals and 91 gaps in the sequential numbering of investigative cases. In response to our audit inquiry, Division management indicated that the gaps resulted from Division employees deleting from ACISS invalid records generated by test submissions, incorrect submissions, and spam submissions. Division employees deleted the records in an effort to exclude invalid records from ACISS data statistical reports. However, Division management also indicated that documentation supporting the reasons for deleting the records had not been maintained and noted that the Division had not established a procedure requiring Division staff to document the reason and approval for deleting referral and investigative case records from ACISS.

Without a record of all referrals and investigative cases deleted from ACISS and documented explanations for the deletions, errors that occur during the submission process may not be appropriately identified and documented and deletions may not be appropriately monitored and approved. As a result, there is an increased risk that referrals and investigative cases may not be properly handled and that documentation of Division actions related to referrals and investigative cases may not be appropriately maintained.

Recommendation: We recommend that Division management establish procedures for documenting the reason and approval for deleting referral and investigative case records from ACISS. These procedures could include the establishment of logs to document and provide an explanation for all referrals and investigative cases deleted from ACISS. If established, such logs should be periodically reviewed by management to determine the significance and nature of data gaps as well as the status of any uncorrected data errors.

Finding 5: ACISS Access Controls

Effective access controls include measures that limit user access privileges to data and information technology (IT) resources in a manner that promotes an appropriate separation of duties and restricts users to only those functions necessary to perform their assigned job responsibilities. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

To ensure security over State agency IT systems and data, minimum security standards were established in Agency for Enterprise Information Technology (AEIT) rules.[10] Those rules specify that agency information owners are responsible for authorizing access to information and require that access be based on the principle of least privilege. The rules also require that a user's access authorization be removed when the user separates from employment or transfers to a position where access to the information resource is no longer required.

The Division used the Department, Division of Information Systems *IT Application Access and Resource Request Form 1820* (Form 1820) to establish user access privileges to ACISS. Department policies and procedures also required the Division's access control administrator to deactivate ACISS user access

[10] AEIT Rules 71A-1.007 and 71A-2.004, Florida Administrative Code. Effective July 1, 2014, Chapter 2014-221, Laws of Florida, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; administrative authority; and administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, of the AEIT to the AST.

privileges when employees separated from Department employment or transferred to a position where the access privileges were no longer required.

As part of our audit, we evaluated Department network and ACISS controls, including procedures for assigning and deactivating user access privileges. Our evaluation disclosed that:

- The Division did not assign ACISS user access privileges based on the principle of least privilege. All Division employees with ACISS user access privileges were granted privileges to view and update any open Division referral or investigative case, including cases to which employees were not assigned. In response to our audit inquiry, Division management indicated they had used the Form 1820 to authorize user access to ACISS; however, we noted that the form did not provide a mechanism to specify the level of access to be authorized and no other mechanism had been established to specify the level of access authorized.
- ACISS did not record the date user access privileges were deactivated and, as a result, the Division was unable to demonstrate whether ACISS user access privileges were timely deactivated upon an employee's separation from Department employment or transfer to a position where access was no longer required. In response to our audit inquiry, Department management provided ACISS and Department network records indicating that, for the 34 employees who, during the period July 2013 through February 2015, separated from Department employment or transferred to a position that did not require user ACISS access privileges, none of the employees' user accounts had been used to access ACISS after the employees' separation or transfer dates.

Absent management's documented authorization of ACISS user access privileges based on the principle of least privilege, the Division cannot demonstrate that the user access privileges are appropriately restricted to those necessary for the accomplishment of user assigned job responsibilities. In addition, maintaining a record of the date user account privileges are deactivated would better demonstrate that ACISS user access privileges were timely deactivated upon an employee's separation from Department employment or transfer to a position where the privileges were no longer required.

Recommendation: We recommend that Division management limit ACISS user access privileges to only those access privileges necessary for the user's assigned job responsibilities. We also recommend that Department management ensure that ACISS user access privileges are timely deactivated upon an employee's separation from Department employment or transfer to a position where the privileges are no longer required and that such deactivation be appropriately documented.

SELECTED ADMINISTRATIVE ACTIVITIES

As part of our audit, we also evaluated selected Department administrative activities and controls, including those related to network access and the Department's collection and use of social security numbers.

Finding 6: Network Authentication Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain security controls related to Department network authentication needed 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 adequate security controls related

to network 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 strengthen certain security controls related to Department network authentication to ensure the continued confidentiality, integrity, and availability of Department data and related IT resources.

Finding 7: Collection of Social Security Numbers

The Legislature has acknowledged in State law[11] that a person's social security number (SSN) was never intended to be used for business purposes. However, over time the SSN has been used extensively for identity verification and other legitimate business purposes.

Recognizing that an SSN can be used to perpetrate fraud against an individual and acquire sensitive personal, financial, medical, and familial information, the Legislature specified[12] that State agencies may not collect an individual's SSN unless the agency is authorized by law to do so or it is imperative for the performance of that agency's duties and responsibilities as prescribed by law. Additionally, State agencies are required to provide each individual whose SSN is collected written notification regarding the purpose for collecting the number. The SSNs collected may not be used by the agency for any purpose other than the purposes provided in the written notification. State law further provides that SSNs held by an agency are confidential and exempt from public inspection and requires each agency to review its SSN collection activities to ensure the agency's compliance with the requirements of State law and to immediately discontinue SSN collection upon discovery of noncompliance.

We noted that the Department had not established Departmentwide written policies and procedures for the collection and use of SSNs, including the review of its SSN collection activities. In response to our audit inquiry, Department management identified 23 areas that collected SSNs and indicated that, for 4 of the 23 areas, the Department did not document that individuals were provided with written notification regarding the purpose for collecting their SSNs. Department management further indicated that 19 of the 23 areas had conducted the statutorily required review of its SSN collection activities. For 5 of the 19 areas identified as having conducted the required review, we requested documentation of the Department's reviews and noted that 3 of the reviews had been conducted in 2007, another review was conducted subsequent to our audit inquiry, and no documentation was available to support the fifth review.

Effective controls, including Departmentwide written policies and procedures regarding the Department's collection and use of individuals' SSNs, and documented periodic assessments of SSN collection activities, would better ensure and demonstrate Department compliance with statutory requirements and reduce the risk that the SSNs may be unnecessarily collected or utilized for unauthorized purposes.

Recommendation: We recommend that Department management establish Departmentwide written policies and procedures regarding the collection and use of individuals' SSNs and take appropriate steps to demonstrate compliance with applicable statutory requirements.

[11] Section 119.071(5)(a)1.a., Florida Statutes.

[12] Section 119.071(5)(a)2.a., Florida Statutes.

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. 2014-103 and 2015-002, and finding No. 4 included in our report No. 2014-020.

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 January 2015 through June 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for 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 focused on the Division of Insurance Fraud (Division) 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 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 Nos. 2014-103 and 2015-002 and finding No. 4 in report No. 2014-020.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

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, regulations, and Division policies and procedures, and interviewed Department personnel to gain an understanding of fraud investigation processes.
- Evaluated the adequacy of Division policies and procedures addressing the processing of referrals from receipt to final disposition.
- Examined Division records for 40 referrals received during the period July 2013 through February 2015 and recorded in the Augmented Criminal Investigative Support System (ACISS) to assess the validity of referral data and the completeness of related ACISS records.
- Examined Division records for 40 referrals closed without investigation during the period July 2013 through February 2015 to determine whether sufficient documentation was maintained to support the Division's decision to close the referrals without investigation.
- Examined 40 Division investigative case files from the population of 3,795 investigative cases closed during the period July 2013 through February 2015 to determine whether the investigations were properly documented in accordance with Division policies and procedures.
- Analyzed data for 3,795 investigative cases closed by the Division during the period July 2013 through February 2015 to identify any cases closed with a disposition of *Closed – Due to Resource Limitations*.
- Analyzed ACISS data related to referrals received by the Division and investigative cases initiated during the period July 2013 through February 2015 to identify gaps in the sequentially numbered records and trends or similarities in referrals and investigations by month and regional office.
- Compared ACISS records for the referrals reported by the Division as received from the Office of Financial Regulation (OFR) during the period July 2013 through February 2015 to an OFR-provided listing of referrals submitted to the Division during the same time period and evaluated the reasons for the differences noted.
- Obtained an understanding of Division evidence controls through inquiry of Division personnel and performed a walkthrough of the Division's evidence vault in May 2015 to determine whether evidence appeared to be appropriately accounted for and safeguarded.
- Obtained an understanding and evaluated the effectiveness of Department user access controls for the network and ACISS, including procedures for granting, changing, and removing employees' user access privileges. For the 34 ACISS users who, during the period July 2013

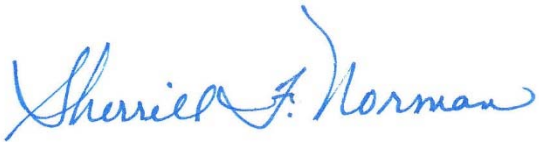
through February 2015, separated from Department employment or transferred to a position that did not require ACISS access privileges, reviewed network and ACISS records to determine whether the users' accounts were timely deactivated and whether the users' accounts were used to access ACISS subsequent to the employees' separation or transfer dates.

- Evaluated Department actions taken to correct the applicable findings noted in our report No. 2014-103. Specifically, we:
  - Evaluated the adequacy of Division of Public Assistance Fraud (DPAF) policies and procedures addressing the documentation of investigations in the Automated Investigation Management System.
  - Determined through inquiry of DPAF management and review of available data analysis reports whether DPAF had performed data analysis procedures, including data mining, to identify potential public assistance fraud.
  - Evaluated DPAF's organizational structure to determine the appropriateness of regional office staffing levels.
  - Examined the personnel files for 10 of DPAF's 67 employees as of February 16, 2015, to determine whether the employees had received appropriate training to facilitate the detection of potential fraud and the performance of investigations.
  - Reviewed the personnel files for 8 of DPAF's 43 investigators as of February 16, 2015, to verify that the investigators possessed the required qualifications.
  - From the population of 3,430 referrals received during the period January 2015 through February 2015, examined DPAF records for 44 referrals to determine the completeness, timeliness, and data validity of the referrals. We also examined DPAF records for an additional 28 referrals to determine whether the records included a reason for rejecting the referrals.
  - Evaluated and assessed the effectiveness of the data analysis tools and techniques implemented by DPAF to detect potential fraud cases.
  - Examined the records for 25 DPAF investigative case files closed during the period July 2013 through February 2015 to determine whether the investigations were properly completed and adequately documented.
  - Through inquiry of DPAF management and examination of DPAF records, evaluated whether the request, issuance, use, and, if applicable, return and disposal of DPAF Electronic Benefit Transfer (EBT) cards during the period July 2013 through February 2015 was adequately documented, as well as whether DPAF conducted monitoring and periodic inventories of the EBT cards.
  - Evaluated DPAF compliance with the State Law Enforcement Bureau (SLEB) agreement and DPAF performance related to its SLEB responsibilities for the period July 2013 through February 2015 by examining documentation submitted to the United States Department of Agriculture Food and Nutrition Service (FNS) related to investigations.
  - For ten EBT cards issued by the FNS to DPAF during the period January 2014 through February 2015 for investigative activities, reviewed documentation of the request for, and approval of the EBT cards, and the DPAF reports submitted to the FNS related to the cards, to evaluate whether appropriate information was included in the requests and reports, and whether appropriate FNS approval was obtained for the cards.
- Evaluated Department actions taken to correct finding No. 4 noted in our report No. 2014-020. Specifically, we reviewed Department records regarding the procurement of a workers' compensation claims system by the Division of Risk Management to determine whether the procurement complied with applicable State laws, rules, and other guidelines.

- Evaluated Department actions taken to correct the applicable findings noted in our report No. 2015-002. Specifically, we:
    - Reviewed Department policies and procedures to obtain an understanding of Department internal controls over the procurement process and examined documentation for selected procurements to determine whether controls were appropriately designed and effectively implemented.
    - Examined Department records for 9 agreements totaling $422,852 selected from the population of 42 agreements totaling $3,375,074 executed utilizing noncompetitive procurement processes during the period August 2014 through March 2015 to determine whether the agreements were reviewed, approved, executed, and monitored in accordance with governing laws, rules, and Department policies and procedures. Additionally, for the 9 agreements we determined whether the applicable contract managers received required contract management training in accordance with State law and whether the Department documented that the contract managers were independent of, and had no conflict of interest in, the entities whose contracts they were assigned to manage.
    - Examined Department records for five payments totaling $150,182, made during the period August 2014 through March 2015 and related to 4 of the 9 selected agreements to determine whether the payments had been properly reviewed and approved.
- From the population of 271 Florida Accounting Information Resource Subsystem (FLAIR) user accounts for Department employees with FLAIR update privileges during the period January 2014 through February 2015, examined FLAIR access control records for 6 FLAIR user accounts to determine whether the access privileges were appropriate given the employees' job duties.
- Compared dates of employment separations with the dates FLAIR user access privileges were deactivated to evaluate the timeliness of the deactivations for the 78 FLAIR user accounts related to 68 Department employees who separated from Department employment during the period January 2014 through February 2015.
- Interviewed Department management, examined selected Department records, and evaluated Department compliance with applicable statutory requirements for collecting and utilizing individuals' social security numbers.
- Observed, documented, and evaluated the effectiveness of selected Department processes and procedures for:
    - Budgetary, cash management, revenue, and cash receipts processes.
    - The administration of Department purchasing cards. As of December 31, 2014, the Department had 1,018 active purchasing cards.
    - The administration of Department travel. Department travel costs totaled approximately $2.6 million during the 2013-14 fiscal year.
    - The acquisition, assignment, and use of wireless devices with related costs totaling approximately $600,000 for the period July 2013 through December 2014.
- 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.

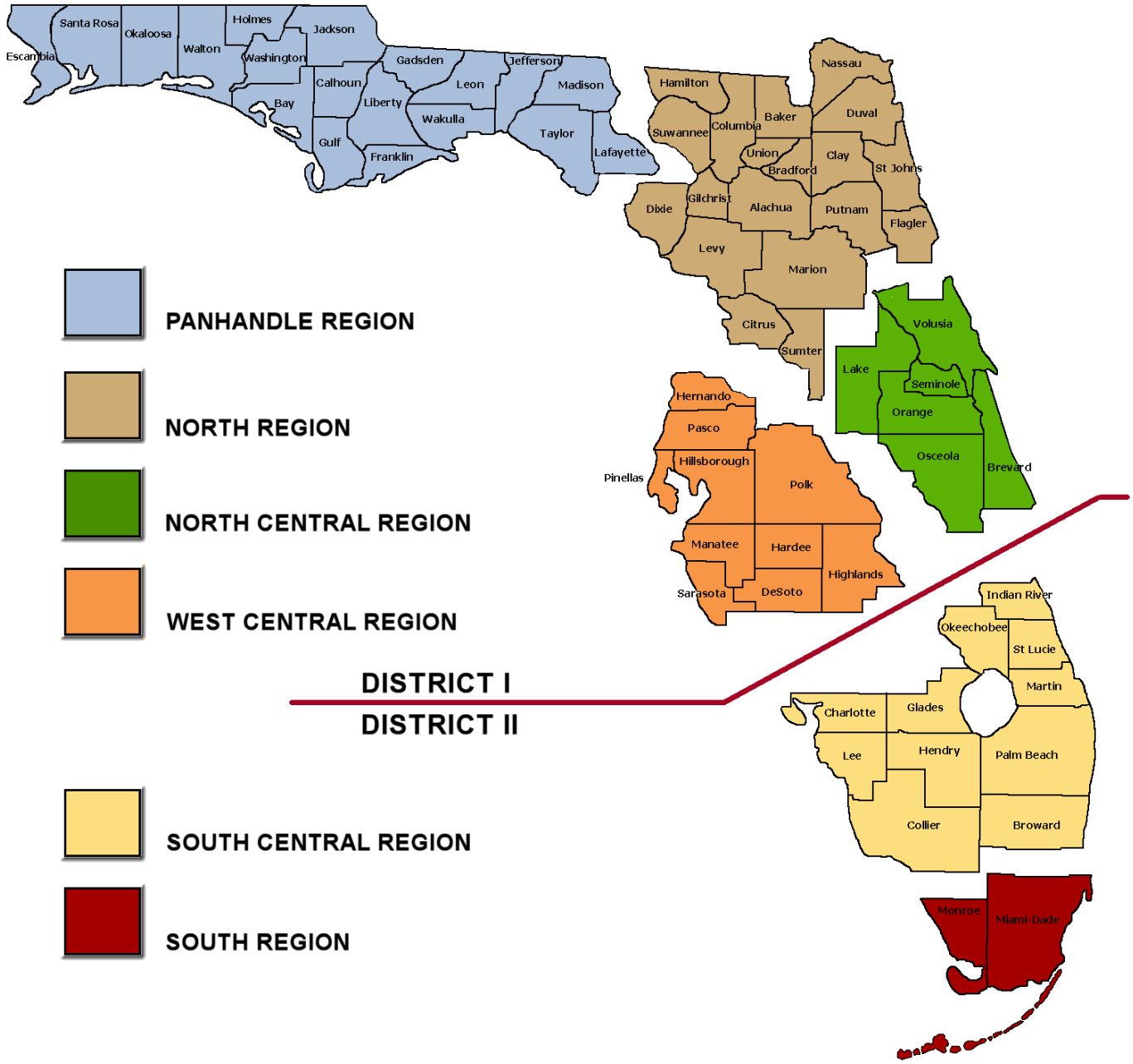


Sherrill F. Norman, CPA
Auditor General

EXHIBIT A

DIVISION OF INSURANCE FRAUD

REGIONAL OFFICES



Source: Division's Web site.



CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

December 21, 2015

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 *Department of Financial Services, Division of Insurance Fraud and Selected Administrative Activities.*

If you have any questions concerning this response, please contact Teresa Michael, Inspector General, at (850) 413-3112.

Sincerely,

Jeff Atwater

JA:rlg

Enclosure

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

DEPARTMENT OF FINANCIAL SERVICES
DIVISION OF INSURANCE FRAUD AND
SELECTED ADMINISTRATIVE ACTIVITIES

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Processing of Referrals

The Division did not always include sufficient information in the Augmented Criminal Investigative Support System (ACISS) to support the reasons referrals regarding potential insurance fraud were closed without investigation.

Recommendation: We recommend that Division management ensure that sufficient information is included in ACISS to support decisions to close referrals without investigation.

Response: Concur. In order to augment and better document the disposition of referrals, the Division will require all personnel to record a detailed explanation for their assessment and closure within the ACISS case file. This requirement will be implemented through policy and included in the ACISS training material.

Expected Completion Date for Corrective Action: Policy change and initial training will be conducted by January 31, 2016.

Finding No. 2: Office of Financial Regulation Referrals

The Division did not ensure that all referrals received from the Office of Financial Regulation (OFR) were identified or accurately recorded in ACISS. In addition, contrary to the Division's Memorandum of Understanding with the OFR, the Department did not provide the OFR with information on the disposition of referrals.

Recommendation: We recommend that Division management ensure that all referrals received from the OFR are accurately identified in ACISS and that referral disposition information is timely reported to the OFR as specified by the MOU.

Response: Concur. As of September 2015, the Division had designated the Bureau Chief of Workers' Compensation Fraud as the point of contact for OFR. The Bureau Chief will acknowledge, track and reply to OFR on all referrals received as well as those submitted to OFR by the Division. The Bureau Chief will be responsible for ensuring that all referrals are properly identified, evaluated and handled by Division personnel. The Bureau Chief will also be responsible for submitting quarterly reports to OFR providing the status and dispositions of all referrals received.

Expected Completion Date for Corrective Action: This process/program was implemented in September 2015.

Finding No. 3: Reasons for Closing Investigations

Division investigations of potential insurance fraud were sometimes inappropriately closed in ACISS using a resource limitations reason code.

Recommendation: We recommend that Division management remove *Closed – Due to Resource Limitations* as a reason code in ACISS for closing investigations. We also recommend that Division management evaluate whether any of the investigations closed using the *Closed – Due to Resource Limitations* reason code should be reopened.

Response: Concur. The Division became aware of this oversight when discovered by the Auditor General in May 12, 2015. The classification was immediately removed from the system to avoid further use by personnel.

Expected Completion Date for Corrective Action: "Closed – Due to Resource Limitations", code was removed May 12, 2015. An audit of all investigations closed under this code will be conducted and all cases will be re-evaluated by January 31, 2016.

Finding No. 4: ACISS Data Processing Controls

ACISS data processing controls need improvement to provide for the proper accounting for and processing of referrals and investigative cases.

Recommendation: We recommend that Division management establish procedures for documenting the reason and approval for deleting referral and investigative case records from ACISS. These procedures could include the establishment of logs to document and provide an explanation for all referrals and investigative cases deleted from ACISS. If established, such logs should be periodically reviewed by management to determine the significance and nature of data gaps as well as the status of any uncorrected data errors.

Response: Concur. In order to improve the control process of deleted referrals and case reports, the Division has implemented a process of logging each spam or created-in-error report deleted. The log tracks the report number, type of report, sub-type of report/offense, status of referral/case, originating authority, date created, reason for deletion, date deleted and deleting authority. Each report will be saved as a PDF file and electronically stored prior to logging and deleting. Only two employees have ACISS authority to delete records. The Operational Support Services Major will conduct audits every 6 months.

Expected Completion Date for Corrective Action: The process of logging deleted records was implemented on July 16, 2015. The storing of PDF files and tracking of audits will begin December 14, 2015.

Finding No. 5: ACISS Access Controls

ACISS controls need improvement to ensure that user access privileges are limited to only those necessary for the user's assigned job responsibilities and to demonstrate that user access privileges are timely deactivated upon an employee's separation from Department employment or when the privileges are no longer required.

Recommendation: We recommend that Division management limit ACISS user access privileges to only those access privileges necessary for the user's assigned job responsibilities. We also recommend that Department management ensure that ACISS user access privileges are timely deactivated upon an employee's separation from Department employment or transfer to a position where the privileges are no longer required and that such deactivation be appropriately documented.

Response: The Division has a process in place designed to quickly and efficiently restrict access to all agency data and information when personnel separate from the agency. To ensure better tracking and documenting of the deactivation process, the Division will start maintaining a log of all personnel separating from the agency and the date their access was rescinded.

The Division is comprised of sworn law enforcement officers, criminal intelligence analysts and administrative support personnel. As a state agency, the Division is responsible for investigating all insurance fraud violations anywhere in the state. All information received and developed is stored in ACISS, making ACISS not only a case tracking system but an extensive intelligence database of all insurance fraud activity occurring in the State of Florida as well as other locations. Experience has shown that the individuals and organizations responsible for committing such crimes often change geographical locations and have links to other criminal elements throughout the state. In order to properly and effectively investigate the referrals received, Division personnel need access to all intelligence information gathered in ACISS. In addition, it is not uncommon for personnel from one field office to provide assistance to other offices on referrals/cases.

Officers, analysts and administrative personnel all have need to operate in the system and make entries or glean information from it. The ACISS system has security features which restrict access to information based on assignment or geographical location. In addition, ACISS has the ability to restrict access to sensitive cases to only those cleared by the overseeing authority. As previously stated, the ability to access information by agency personnel throughout the state is a critical function of the Division. Although employees do have the ability to see information entered in the system, they are unable to update or change any information or reports entered by another member. ACISS only allows information to be entered through the creation of reports which must be reviewed and approved by a supervisor or system administrator.

The Division will update its access control procedures and position descriptions, as necessary, to clearly establish the level of access needed for each position type. In addition, the Division will work with the Division of Information Systems to update the Form 1820 to identify the levels of access for the ACISS system and further ensure that system logs are routinely reviewed to ensure that access to case files is properly monitored.

Expected Completion Date for Corrective Action: March 30, 2016

Finding No. 6: Network Authentication Controls

Certain security controls related to Department network authentication need improvement to better protect the confidentiality, integrity, and availability of Department data and information technology resources.

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

Response: The Department is conducting comprehensive assessments of controls, including related monitoring. We are actively increasing our security account monitoring and deploying account credential protections.

Expected Completion Date for Corrective Action: Monitoring should be in place by July 1, 2016. Account credential protection will be in place by the end of 2016.

Finding No. 7: Collection of Social Security Numbers

The Department had not established Department-wide policies and procedures for the collection and use of social security numbers or always documented the timely evaluation of its collection and use of social security numbers to ensure compliance with State law.

Recommendation: We recommend that Department management establish Department-wide written policies and procedures regarding the collection and use of individuals' SSNs and take appropriate steps to demonstrate compliance with applicable statutory requirements.

Response: Concur. The Division of Administration will work with the Division of Legal Services to develop a Department-wide policy to address the collection of social security numbers. The policy will require and provide for the timely evaluation of the collection and use of social security numbers by the various divisions, bureaus and offices to ensure Department-wide compliance with State law. The Division of Administration, Division of Agent and Agency Services, Division of Public Assistance Fraud and Division of Accounting and Auditing will review its current practices for the collection of social security numbers to ensure compliance with statutory requirements. The Division of Workers' Compensation, State Fire Marshal and Division of Treasury reviewed their practices for the collection of social security numbers and revised/implemented procedures to ensure compliance with the applicable statutory requirements.

Expected Completion Date for Corrective Action: February 2016